Symantec™ Intruder Alert 3.6.1 Administration Guide

symantec™

Symantec Intruder Alert 3.6.1 Administration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 3.6.1.

Copyright Notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
    - Error messages/log files
    - Troubleshooting performed prior to contacting Symantec
    - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country and then choose Service and Support.

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Section 1 Getting Started

Chapter 1 Introducing Intruder Alert

Chapter 2 Touring Intruder Alert

Chapter 5 Managing Agents

Section 3 Securing systems

Chapter 6 Policies, rules, and criteria

Chapter 7 Administering policies

Chapter 8 Creating and modifying policies

Chapter 9 File and directory security

Chapter 10 Event context capturing

Section 5 Appendices

Appendix A Contacting customer support

Appendix B Operating system collectors

Appendix C ita.ini file documentation

Appendix D Optimization and problem solving techniques

Appendix E SNMP for Intruder Alert

Appendix F Destination ports for Intruder Alert

Section 1

Getting Started

This section introduces you to Intruder Alert as follows:

Chapter 1

Introducing Intruder Alert

This chapter includes the following topics:

Contents and organization of this guide

Section 1: Getting started

The *Getting started* section of the guide contains:

- Chapter 1, “Introducing Intruder Alert”
  This chapter defines Intruder Alert, including each component in its architecture, and briefly describes how each component works together to secure your network.
- Chapter 2, “Touring Intruder Alert”
  This chapter takes you on a screen by screen tour of the Intruder Alert Administrator and Event Viewer.

Section 2: Administering security

The *Administering security* section of the guide contains:

- Chapter 3, “Post-installation options”
  This chapter provides an in-depth tutorial of basic post-installation configuration options available for UNIX and Windows.
- Chapter 4, “Administering Intruder Alert”
  This chapter contains the advanced concepts and instructions for administering Intruder Alert on your network. Administration information includes an overview of user management, post installation options, and basic tasks associated with Manager administration.
- Chapter 5, “Managing Agents”
  This chapter contains advanced concepts and instructions for managing Agents on your network. Administration information includes practical tutorials on basic tasks associated with Agent management and policy administration.

Section 3: Securing systems

The *Securing systems* section of this guide contains:

- Chapter 6, “Policies, rules, and criteria”
  This chapter teaches you how policies, rules, and rule criteria function. It describes Intruder Alert’s select, ignore, and action criteria. Reading this chapter is required for those who plan to create or modify Intruder Alert policies.
- Chapter 7, “Administering policies”
  This chapter provides instructions on how to administer policies in Intruder Alert. Administration tasks include: activating, deactivating, exporting, importing, modifying, and removing policies.
- Chapter 8, “Creating and modifying policies”
  In this chapter you will learn the policy development process. The chapter’s examples and step-by-step tutorials will help you learn how to create your own policies in Intruder Alert.
- Chapter 9, “File and directory security”
  This chapter teaches you how to monitor “mission critical” files for any changes or movements and how to secure the files and directories on your network.
- Chapter 10, “Configuring event context capturing”

This chapter describes event context capturing, a feature that allows the Agent to remember certain events and use them for selective intrusion detection.

Section 4: Monitoring events

The *Monitoring events* section of this guide contains:

- Chapter 11, "Using Intruder Alert Event Viewer"
  This chapter teaches you the basics of using Intruder Alert Event Viewer to define queries and generate online views.
- Chapter 12, "Generating and viewing reports"
  This chapter describes Intruder Alert's report generation and viewing capabilities. You will learn about the various security and status reports and how to generate them.

Appendices

This guide contains the following appendices:

- Appendix A, "Contacting customer support"
  This appendix describes where users can turn for help when using Intruder Alert.
- Appendix B, "Operating system collectors"
  This appendix discusses how Intruder Alert collects events on UNIX and Windows operating systems.
- Appendix C, "ita.ini file documentation"
  This appendix discusses the ita.ini file.
- Appendix D, "Optimization and problem solving techniques"
  This appendix describes how to optimize various aspects of your system's performance, such as managing Intruder Alert's bandwidth and disk space usage.
- Appendix E, "SNMP for Intruder Alert"
  This appendix describes how to install and use SNMP services. The SNMP services allow Intruder Alert to send and receive SNMP traps.
- Appendix F, "Destination ports for Intruder Alert"
  This appendix describes the destination ports used by each component of Intruder Alert.

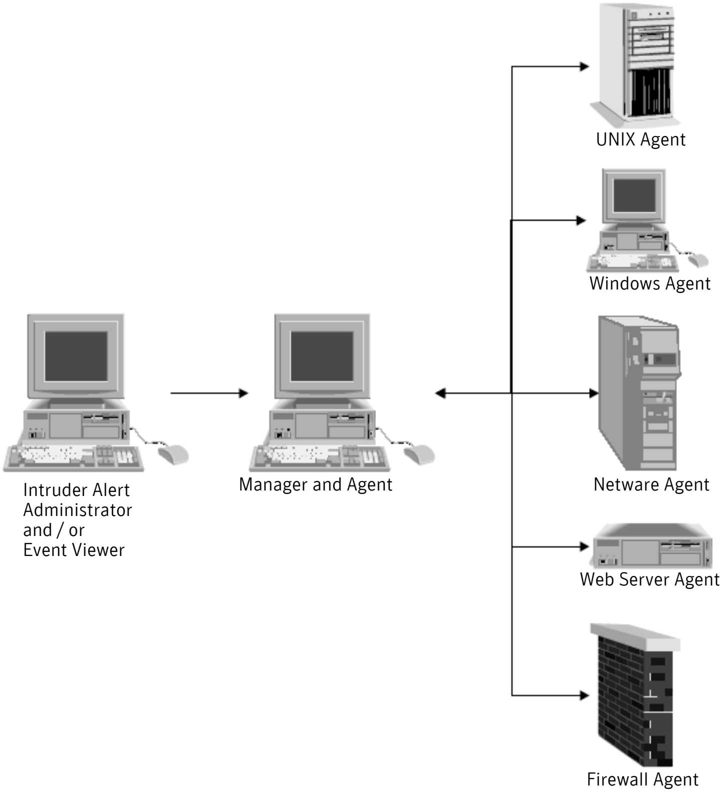
Understanding Intruder Alert's architecture

The architectural components of Intruder Alert include:

- Administrator
- Event Viewer
- Manager
- Agent

The following graphic illustrates Intruder Alert's architecture.

Figure 1-1 Intruder Alert Architecture



The Intruder Alert Administrator

Intruder Alert Administrator provides a Windows graphical user interface (GUI) that serves as Intruder Alert's administrative console. Using Intruder Alert Administrator, you will:

- Connect to and disconnect from Managers
- Organize and configure Agents
- Create and manage domains
- Create and administer policies
- Manage Intruder Alert users and user privileges

Intruder Alert Administrator contains the master list of Drop & Detect™ and Configure to Detect policies. Drop & Detect-Install policies are applied during installation with no configuration required. Drop & Detect-Miscellaneous and Configure to Detect policies require either system or policy configuration. All Intruder Alert out-of-box policies reside in the Policy Library.

Intruder Alert Administrator supports an unlimited number of Managers. Depending on your network architecture, and the geographic diversity of your organization, you may need to install only one or two Intruder Alert Administrators.

See "Introducing Intruder Alert" on page 15.

The Intruder Alert Event Viewer

Intruder Alert Event Viewer is a separate Windows GUI for viewing event data captured by Agents. When directed (via the Record to Event Viewer action), Agents record events in an event database located on the Manager system. Using Intruder Alert Event Viewer, you will:

- Query a Manager's event database to view selected events as they happen or as a historical snapshot
- Send Intruder Alert commands to Agents
- Generate and view various types of online and printed reports

The Query Builder wizard makes it easy to define, query, or generate online and printed reports.

See "Using the Query Builder wizard" on page 176.

The Intruder Alert Manager

The Manager is a software application that runs on UNIX or Windows. The Manager does not have a graphical user interface. Managers perform the following functions:

- Maintain secure communications with all registered Agents
- Maintain the master list of domains and policies applied to each Agent
- Communicate domain and policy changes to Agents
- Receive and store event data from Agents (via the Record to Event Viewer action)
- Serve as the communication link between Intruder Alert Administrator, Intruder Alert Event Viewer, and Agents
- Maintain the list of policies, and the domains to which they are applied

The Manager does not require a dedicated machine or server. However, it should reside on a fast, stable, secure machine. During installation, Intruder Alert creates platform-specific domains based on the selected policies.

Intruder Alert automatically places a new Agent in one of the following default domains.

- Default—All Agents
- Default—UNIX
- Default—Windows
- Default—Netware

During installation, you can select the UNIX and Windows Drop & Detect policies to be applied to these default domains. After installation, you can use Intruder Alert Administrator to create additional domains and activate additional policies as needed.

For Windows systems, copy any Windows policies that you want to apply in a domain from either the Drop & Detect- Misc. or Configure to Detect branch in the Policy Library.

Note: The total number of Agents capable of registering to a single Manager varies by number of events, operating system, memory, and disk space.

Agents are organized into domains and may belong to more than one domain, if directed. Once a policy has been applied to a domain, the Manager delivers it to the specified Agents. In turn, Managers receive event data from Agents, and store it in an event database. The event database consists of two types of files: an extent (.ext) file and a rex file. For events to be written to the event database, they must be recorded to the Event Viewer.

Rex Files

Rex files contain the most recent events. When the rex file reaches its maximum size (2 MB), the system converts the file from a rex file to an extent file.

Extent Files

Extent files are archived rex files. Only one rex file exists on the Manager at any one time. For example, at install, the system begins with 1.rex. When this file reaches 2 MB, the Manager saves the file as 1.ext and creates 2.rex. When 2.rex becomes full, it saves the file as 2.ext and creates 3.rex.

The Manager can have up to 99,999,999 extent files (i.e., 1.ext through 99999999.ext). The Intruder Alert Event Viewer queries these files for selected data. You can archive this data and delete it from your system if desired.

More information on archiving and managing these files is available.

See "Understand and manage the event database" on page 261.

The Intruder Alert Agent

The Agent is a UNIX daemon or Windows service. Every supported UNIX and Windows system in the network should have an installed Agent.

Agents perform the following services:

- Monitor event collectors
- Perform actions (e.g., notify user, send email, page administrator, etc.)
- Receive policy updates from the Manager
- Establish secured communication with the Manager and encrypt data for transmission across the network

Security events are captured differently on each operating system:

- On UNIX systems, by default the Agent captures events from syslog, wtmp, process accounting and, where available, btmp, btmps, wtmps, and C2 audit logs.
  Intruder Alert must be configured manually to monitor C2 audit logs.
  See "Configure Intruder Alert to monitor C2 collector" on page 224.
- On Windows systems, the Agent captures events from the System, Application, and Security logs.

- Intruder Alert for UNIX and Windows can also be configured to monitor any ASCII audit log.

  See "Configuring external audit log monitoring" on page 85.

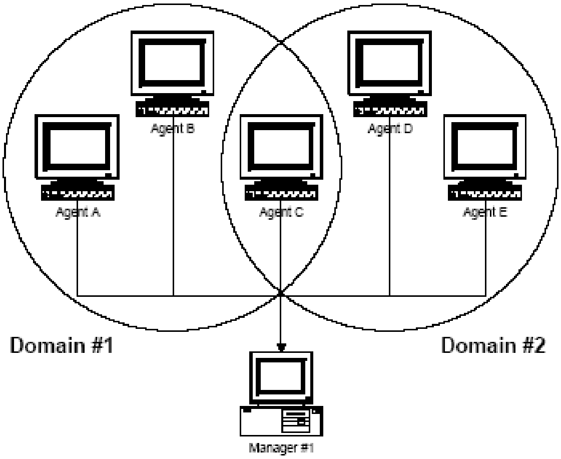
  More information about how events are logged on UNIX and Windows operating systems is available.

  See "Operating system collectors" on page 221.

Agent Domains

Agents are grouped in domains by operating system, location, workgroup, or access restrictions. A domain may contain one or more Agents. In addition, Agents may belong to more than one domain, as illustrated below.

Figure 1-2 Shared Agent Diagram



A Manager may have one or several domains. If desired, each registered Agent may reside in its own domain.

The Manager stores the policy and domain information. Once a policy has been applied to a domain, the Manager delivers that policy to all the Agents in that domain. Agents run the policies 24 hours a day, 7 days a week.

See "Managing Agents" on page 75.

Intruder Alert policies

Policies define which system events to select, which to ignore, and which actions to perform. Intruder Alert comes with pre-configured policies that can be applied during installation.

Policies contain rules and rule criteria that Intruder Alert uses to detect and respond to information security threats.

Rules

A rule is comprised of three parts:

- Select criteria
- Ignore criteria
- Action criteria

All three parts do not have to exist to have a valid rule.

The Select criteria defines the event to detect. The conditions set in the Ignore criteria define exceptions to the rule (if these conditions are present, no actions will be taken). The Action criteria specifies the action to be executed when the Select criteria is met.

Rules can be linked together to detect sequential events. They can be assigned one of the following threat level values:

- Emergency: These rules indicate the highest threat level.
- Alert: These rules indicate a moderate threat level.
- For Your Information (FYI): These rules indicate the lowest threat level.

See “Policies, rules, and criteria” on page 91.

See “Administering policies” on page 127.

Touring Intruder Alert

This chapter includes the following topics:

Intruder Alert Administrator

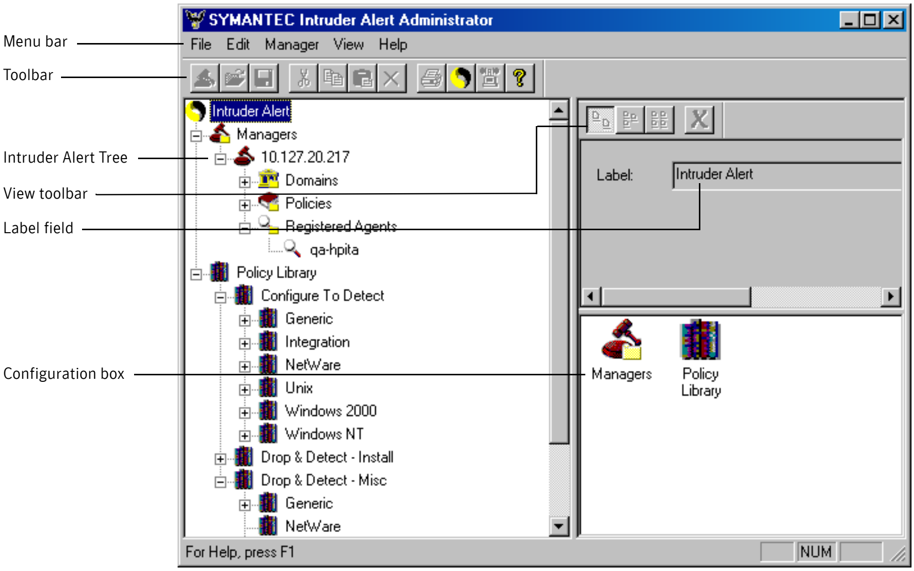
The administration tasks of Intruder Alert have been simplified by using a Graphical User Interface (GUI) for the Intruder Alert Administrator. This section discusses the various tools, objects, and features available in the GUI.

The Intruder Alert Administrator serves as Intruder Alert's command center. It is used to:

- Organize Agents in domains
- Create and apply policies to domains
- Import polices from the Symantec Web site
- Export policies
- Configure Agents for email and paging notification
- Configure Intruder Alert to monitor additional audit logs
- Manage user privileges

Figure 2-1 depicts the Intruder Alert Administrator.

Figure 2-1 Intruder Alert Administrator



See “Starting Intruder Alert Administrator” on page 63.

See “Connecting to a Manager” on page 64.

Once connected to a Manager, you can use the various views and tools available to enable security policies on your network. You can also create and manage reports generated by the Intruder Alert Event Viewer.

After connecting, Intruder Alert Administrator stores the Manager’s name in the Manager’s branch of the Intruder Alert tree, allowing you to view the domains, policies, and registered Agents associated with that Manager.

Menu bar

The menu bar contains five menus: File, Edit, Manager, View, and Help.

Note: With the exception of the Help menu, the availability of all menu items depends upon your location in the program, the selected tree item, and what you are trying to accomplish.

File menu

The File menu contains the following commands:

Table 2-1 File menu commands

Command	Description
New	Create new items
Save	Save any changes you make
Print	Output information to a network printer
Printer Setup	Specify a default printer
Print to File	Output information to a text file
Connect to Manager	Connect to a Manager
Import Policy	Import a policy from your backup directory
Export Policy	Export a policy file to your backup directory

Edit menu

The Edit menu contains the following commands:

Table 2-2 Edit menu commands

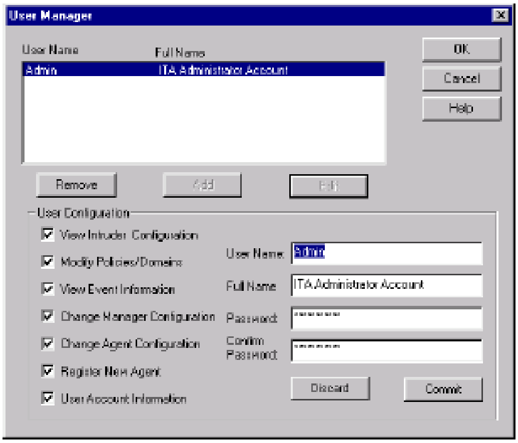
Command	Description
Copy	Copy available items
Cut	Cut available items
Paste	Paste items into appropriate areas
Delete	Delete available items
Reload	Reset any changes made to a policy, or restore a policy to its original unedited version

Manager menu

The Manager menu lets you access the configuration dialog box for the following functions:

Security: Access the User Manager dialog box:

Figure 2-2 Intruder Alert Administrator User Manager Menu



User Name	Full Name
Admin	ITA Administrator Account

User Configuration

- ☑ View Intruder Configuration
- ☑ Modify Policies/Domains
- ☑ View Event Information
- ☑ Change Manager Configuration
- ☑ Change Agent Configuration
- ☑ Register New Agent
- ☑ User Account Information

User Name: Admin

Full Name: ITA Administrator Account

Password: ********

Confirm Password: ********

Paging: Display a list of Agents that are configured to allow paged notifications

Licensing: Enter updates to your license key

View menu

The View menu allows you to activate the following options:

Table 2-3 View menu options

Option	Description
Toolbar	Application menu items displayed graphically
List Toolbar	Control the configuration frame display
Select Toolbar	Rule editing tools
Ignore Toolbar	Rule editing tools
Action Toolbar	Rule editing tools

Help menu

Access the following information through the Help menu:

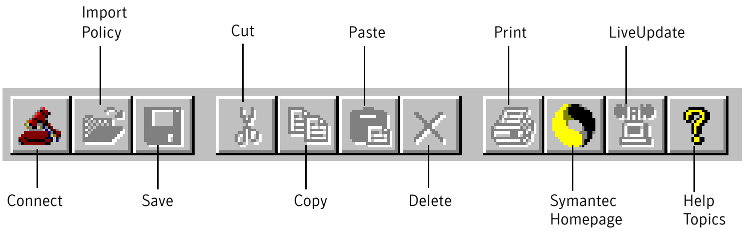
Table 2-4 Help menu topics

Topic	Description
Contents & Index	Access to online help
Go to Homepage	Access to Symantec's home page on the World Wide Web
About Intruder Alert Administrator	Displays the Intruder Alert Administrator version number, and build date

Toolbar

The toolbar contains the most common functions of the Intruder Alert Administrator. Place the pointer over each button to learn its name.

Figure 2-3 Intruder Alert Administrator toolbar



The following list provides the name and function of each button:

Connect — Displays the Intruder Alert Connect to Manager dialog box, allowing you to establish a connection between the Administrator and the Manager.

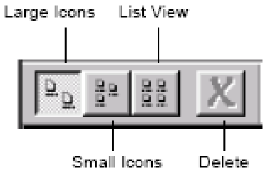
Import Policy — Displays the Import dialog box, allowing you to import a policy.

💾	Save	Saves changes made in the Intruder Alert Administrator. The save button is activated when changes need to be saved.
✂	Cut	Removes the selected object from the tree.
⎘	Copy	Makes a duplicate copy of the selected object.
📋	Paste	Inserts the cut or copied object beneath the selected node.
✕	Delete	Deletes the selected item from the tree.
🖨	Print	Prints information about a policy, rule, or rule criteria.
●	Symantec Homepage	Connects you to the Symantec Web site.
	LiveUpdate	LiveUpdate is no longer used to provide Intruder Alert patches. Instead, go to the Symantec Web site to download updated versions: http://www.symantec.com/techsupp/enterprise/
?	Help Topics	Accesses online help. In online help, the user can browse, or search by keywords.

List toolbar

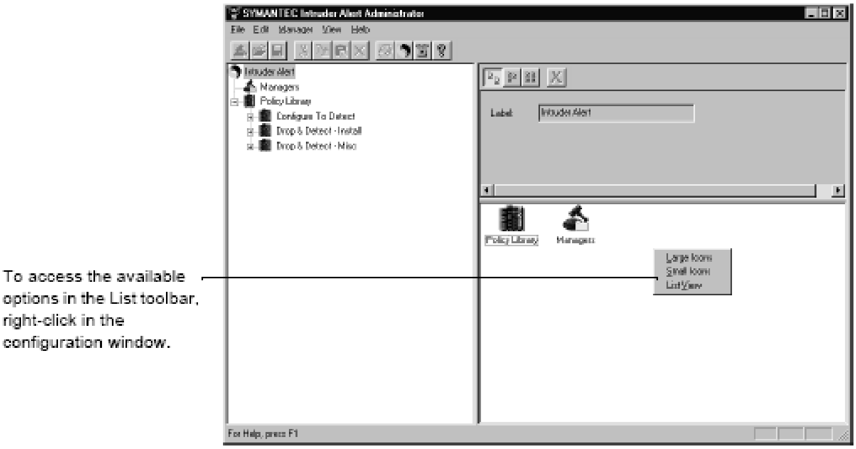
The List toolbar allows you to control the size and placement of the icons in the configuration frame. It appears above the Label field, and may be selected and deselected through the View menu.

Figure 2-4 List toolbar



The functions this bar represents may also be accessed by right-clicking in the configuration frame and using the shortcut menu.

Figure 2-5 Click-access to the List toolbar options



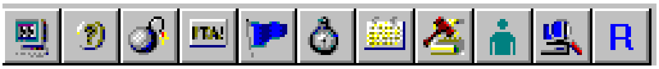
Label: Intruder Alert

To access the available options in the List toolbar, right-click in the configuration window.

Select toolbar

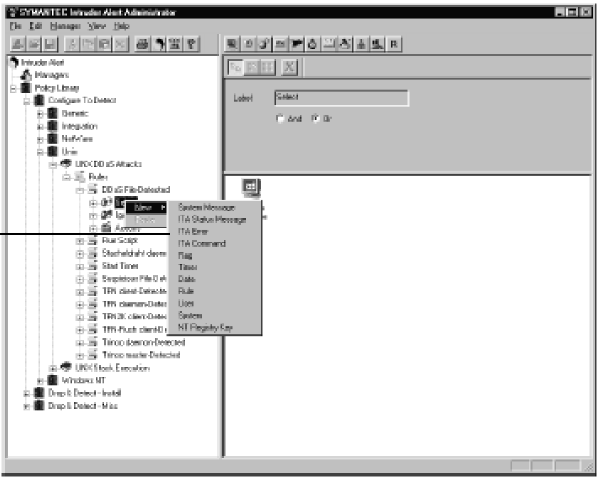
The Select toolbar lets you add Select criteria to a rule with a click of the mouse. The bar is available when creating or editing the Select criteria of a policy rule and may be selected through the View menu.

Figure 2-6 Select toolbar



Select criteria may also be added to rules by right-clicking on the Select node in the tree view as illustrated below.

Figure 2-7 Click-access to the Select toolbar



Label: Select

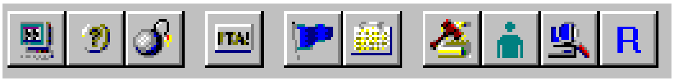
○ And ● Or

To access the available options in the Select toolbar, right-click on the Select node in the tree view.

Ignore toolbar

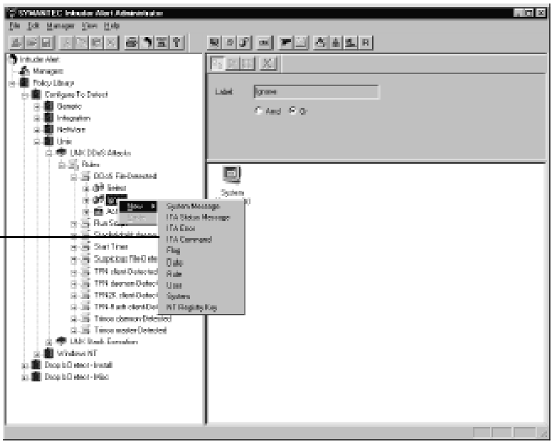
The Ignore toolbar lets you add Ignore criteria to the rule with a click of the mouse. The bar is available when creating or editing the Ignore criteria of a policy rule, and may be selected in the View menu.

Figure 2-8 Ignore toolbar



Ignore criteria may also be added to rules by right-clicking on the Ignore node in the tree view as illustrated below.

Figure 2-9 Click-access to the Ignore toolbar



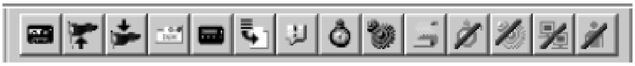
Label: Ignore
○ And ● Or

To access the available options in the Ignore toolbar, right-click on the Ignore node in the tree view.

Action toolbar

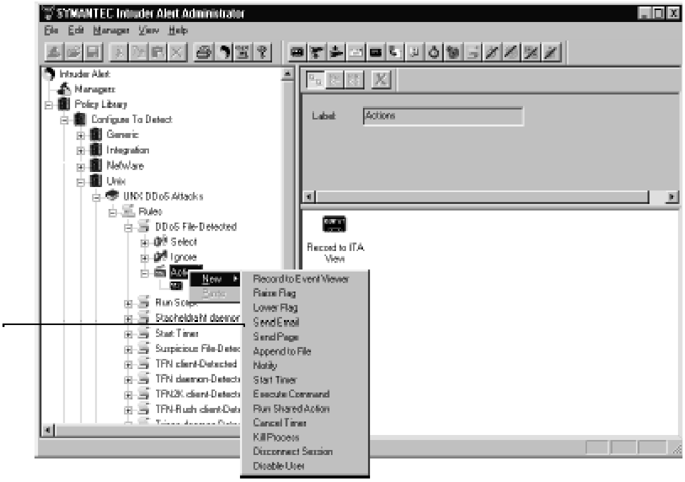
The Action toolbar lets you add an action to the rule with a click of the mouse. The bar is available when creating or editing a policy rule action, and may be selected in the View menu.

Figure 2-10 Action toolbar



An Action may also be added to rules by right-clicking on the Action node in the tree view as illustrated below.

Figure 2-11 Click-access to the Action toolbar



To access the available options in the Action Toolbar, right click on the Action node in the tree view.

Select and Ignore criteria

The following is a list and description of the Select and Ignore criteria available in Intruder Alert:

Table 2-5 Select and Ignore criteria

Criteria	Description
System Message	Selects or ignores specific text in event messages generated by an application or operating system.
ITA Status Message	Selects or ignores specific text in Intruder Alert status messages.
ITA Error	Selects or ignores specific text in Intruder Alert error messages.

Table 2-5 Select and Ignore criteria

Criteria	Description
ITA Command ITA!	Selects or ignores Intruder Alert commands sent to the Agent from Intruder Alert Event Viewer.
Flag	Selects or ignores flags raised by other rules.
Timer (Select only)	Selects timers started by another rule's action.
Date	Selects or ignores events occurring within a range of time.
Rule	Selects or ignores a specified rule.
User	Selects or ignores events generated by specific users.
System	Selects or ignores events generated on specific Agent systems.
Registry Key R	Selects or ignores events generated by the Windows registry.

Rule Actions

The following table defines the actions available for use in policy rules:

Table 2-6 Actions

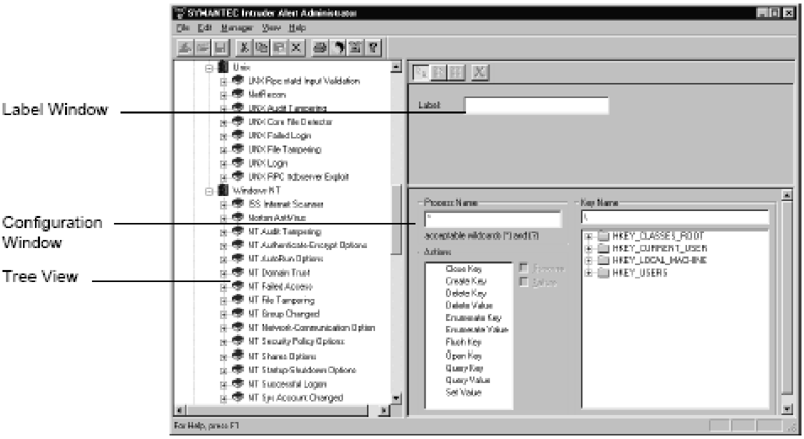
Action	Description
Record to Event Viewer	Records the event in an event database on the Manager system for Intruder Alert Event Viewer reporting. This is the default action for all Drop & Detect policies.
Raise Flag	Raises a flag for a specified period of time. The flag can be selected by another rule.
Lower Flag	Cancels a raised flag.
Send Email	Emails the event message to a specified recipient.
Send Page	Notifies an administrator via pager that an event occurred.
Append to File	Notifies an administrator via pager that an event occurred.
Notify	Sends the event message and, if desired, a user-defined message to a user or host.

Table 2-6 Actions

Action	Description
Start Timer	Initiates a timer to count down to a specified date or for a specified amount of time.
Execute Command	Executes a system command, batch file, executable file, or shell script, depending on the type of operating system.
Run Shared Action	Executes an action defined in another policy rule residing on the Agent system.
Cancel Timer	Terminates a timer.
Kill Process	Stops the process referenced in the event.
Disconnect Session	Disconnects the user's session.
Disable User	Disables a user's account (except for an account having root, administrator, or supervisor privileges).

Intruder Alert Administrator fields

Figure 2-12 Intruder Alert Administrator fields



The different fields are described as follows:

- Label field

  Located in the right pane, in the top section of the Administrator, the label field provides information to identify the name of the application item that is selected in the Configuration frame. It may also display an input field or activation check box for certain selected items.

- Configuration frame

  This frame contains configuration dialogs for various Intruder Alert elements.

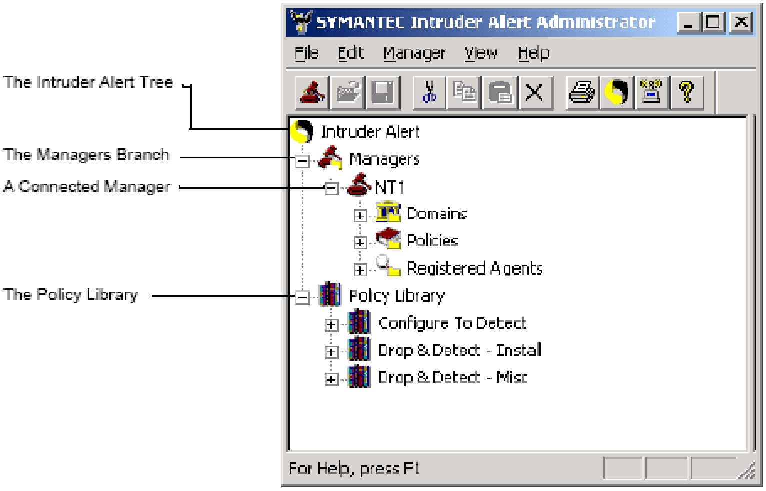
- Intruder Alert tree

  Located in the left pane, the Intruder Alert tree simplifies the process of administering Intruder Alert.

Intruder Alert tree

The following graphic illustrates the main branches of the Intruder Alert tree.

Figure 2-13 Intruder Alert tree



In the Intruder Alert tree there are two main branches, the Managers branch and the Policy Library branch—hereafter referred to as the Policy Library.

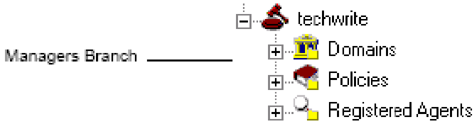
The Managers branch lists the available Managers, and all domains, policies, and registered Agents belonging to each Manager.

The Policy Library contains all the policies that ship with Intruder Alert as well as user defined policies.

Managers branch

The Managers branch lists all connected Managers. The name of the Manager appears in the tree once the Administrator has established a connection to that Manager. The Administrator allows you to connect to multiple Managers at the same time. Managers not currently connected to the Administrator appear with a red mark across the Manager icon. Listed beneath each Manager are a number of domains, policies, and registered Agents, as shown in the following illustration.

Figure 2-14 Managers branch



Managers can have as many as 100 registered Agents reporting to them, although this varies by operating system type.

Domains

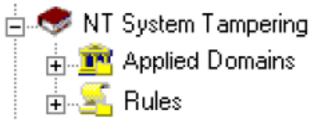
When Agents are installed, they are initially organized into default domains. The Domains branch lists the Agent domains available on a given Manager. Each domain contains two subbranches:

- Policies in Domain
  The Policies in Domain branch lists the policies applied to the Agent domain.
- Agents in Domain
  The Agents in Domain branch lists the Agents assigned to the selected domain.

Policies

The Policies branch lists all policies applied to a Manager. The policies that were applied at the time of installation are located in this branch. You can copy policies from the Policy Library into this branch, and apply them to a domain. When a policy is removed from a domain, it still resides in the Policies branch. The Applied Domains and Rules branches appear beneath each policy.

Figure 2-15 Applied Domains and Rules branches



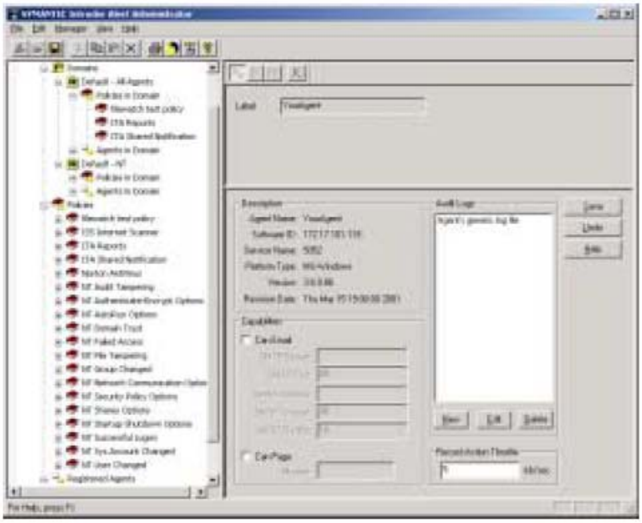
The branches are described as follows:

- Applied Domains
  The Applied Domains branch lists the domains on which the policy is applied.
- Rules
  The Rules branch lists the rules for the selected policy. Rules specify which events to detect and actions to perform.

Registered Agents

The Registered Agents branch lists all Agents registered to a selected Manager. When an Agent is selected, the Agent configuration fields appear in the configuration frame in the right pane of the Administrator window.

Figure 2-16 Agent configuration fields



The Agent configuration fields are used to:

- Set up the Agent with email and paging capabilities
- Configure additional audit logs for Agents to monitor
- Throttle the rate Agents record events in the Manager’s event database

Policy Library

The Policy Library is the second primary branch in the Intruder Alert Administrator Tree. It contains all the out-of-box policies and serves as the repository for any user-defined policies.

Intruder Alert’s out-of-box policies are grouped into three categories:

- Drop & Detect-Install
- Drop & Detect-Misc
- Configure to Detect

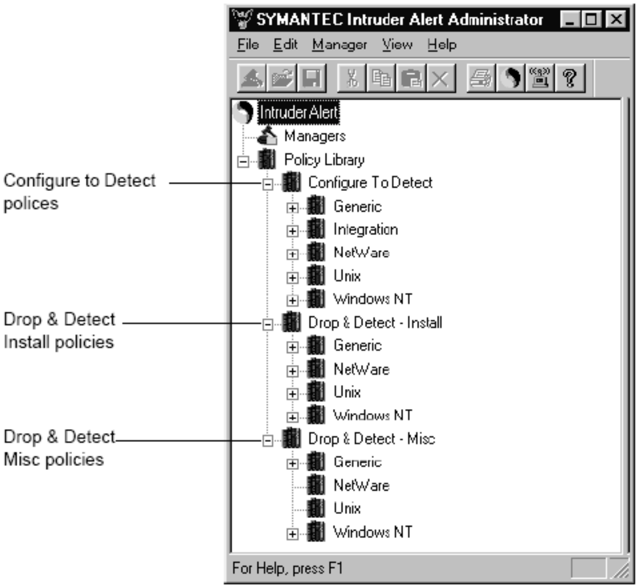
Most Drop & Detect policies are selected and applied at the time of installation. They require no configuration and only need to be applied to a domain.

Drop & Detect-Misc policies are not selectable during installation and can only be installed after everything is configured. Drop & Detect-Misc policies are used for debugging, diagnostics, troubleshooting, and protecting the system.

Configure to Detect policies require system or policy configuration to function. Contact a Symantec consultant for assistance in configuring and activating these policies.

You can also create and store your own policies in the Policy Library. The following graphic illustrates how these policies are organized.

Figure 2-17 The Policy Library



Intruder Alert Event Viewer

The reporting features of Intruder Alert have been simplified by using a Graphical User Interface (GUI) for the Intruder Alert Event Viewer. This section discusses the various tools, objects, and features available in the GUI.

The Intruder Alert Event Viewer is used to view event data captured by Agents. When directed (via the Record to Event Viewer action), Agents record events in an event database located on the Manager's system.

The Intruder Alert Event Viewer runs only on Windows.

Using the Intruder Alert Event Viewer you can:

- Query a Manager's event database and view selected events as they happen or view historical snapshots of the data
- Send Intruder Alert commands to Agents

- Generate and view various reports

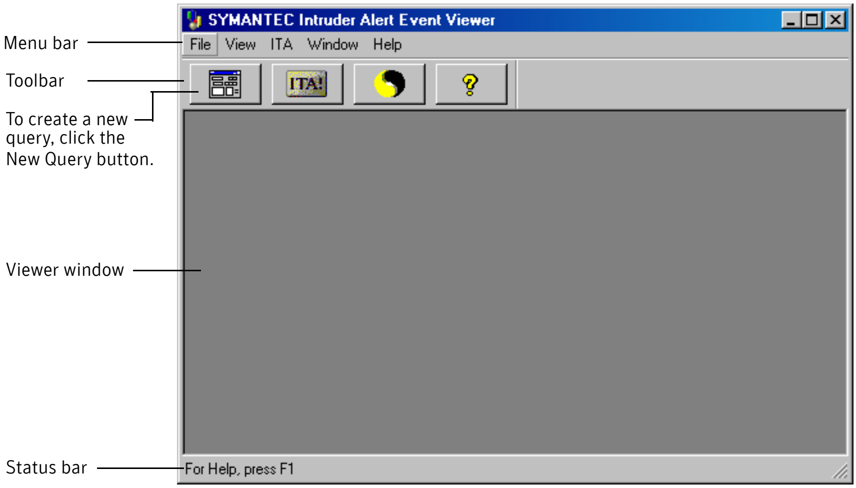
To begin using the Intruder Alert Event Viewer

1 Launch the Event Viewer by doing one of the following:

  - Launch the Event Viewer from the Windows Start menu.
  - Click the application icon on the Windows desktop.

The Event Viewer consists of a viewer window bordered on the bottom by a general information status bar, and headed by two general command elements, the menu bar and toolbar.

Figure 2-18 Intruder Alert Event Viewer


SYMANTEC Intruder Alert Event Viewer
File View ITA Window Help
ITA!
Menu bar
Toolbar
To create a new query, click the New Query button.
Viewer window
Status bar
For Help, press F1

Note: If you maximize the task window, you must choose a cascade or tile view in order to view additional task windows that may be open in the background.

Menu bar

The Event Viewer menu bar contains five menus: File, View, ITA, Window and Help.

Note: With the exception of the Help menu, the availability of all menu items depends upon your location in the program, the selected tree item, and what you are trying to accomplish.

File menu

Depending on the context, the File menu may contain any of the following commands:

Table 2-7 Event Viewer File menu commands

Command	Description
New Query	Create a new query, and define the view type
Load View	Open a custom view that is linked to a particular Manager
Save View	Save a custom view This option allows the query to be saved with Manager specific information. It is only available after a view has been created, and is open on the viewer desktop.
Load Generic View	Open a generic view that can be applied to any Manager
Save Generic View	Save a custom generic view This option allows the query to be saved without Manager specific information. It is only available after a view has been created, and is open on the viewer desktop.
Print	Output information to a default printer
Print Setup	Specify a default printer
Exit	Exit from the viewer

View menu

The View menu allows you to activate and deactivate the following features of the Intruder Alert Event Viewer.

Table 2-8 Event Viewer View menu options

Option	Description
Toolbar	Display or remove the toolbar
Status Bar	Display or remove the status bar

ITA menu

The ITA menu contains a single command.

Table 2-9 Event Viewer ITA menu command

Command	Description
Send Intruder Alert Command	Trigger a user-defined rule

Window menu

The Window menu allows you to activate several task display options on the Event Viewer desktop.

Table 2-10 Event Viewer Window menu display options

Display option	Description
Cascade	Create a cascading display of all open task windows in order of activation
Tile	Create a tiled display of all open task windows
Arrange Icons	Arrange minimized report windows in order of most recent report. It also rearranges the minimized windows after you have resized the general Event Viewer desktop.

Help menu

Through the Help menu you can access several sources of information.

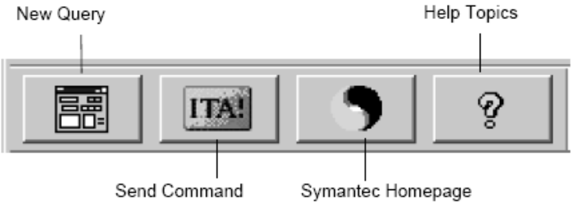
Table 2-11 Event Viewer Help menu options

Option	Description
Help topics	Assistance with Intruder Alert features
Go to Homepage	Support on the Web
About Intruder Alert Event Viewer	Display the Event Viewer version and build date

Toolbar

The toolbar allows you to launch routine tasks with a single click of the button.

Figure 2-19 Intruder Alert Event Viewer toolbar



The tasks available on the toolbar include:

- Define a new query
- Send an Intruder Alert command

In addition, the toolbar provides access to Symantec's Web site and online help.

Event Viewer task features

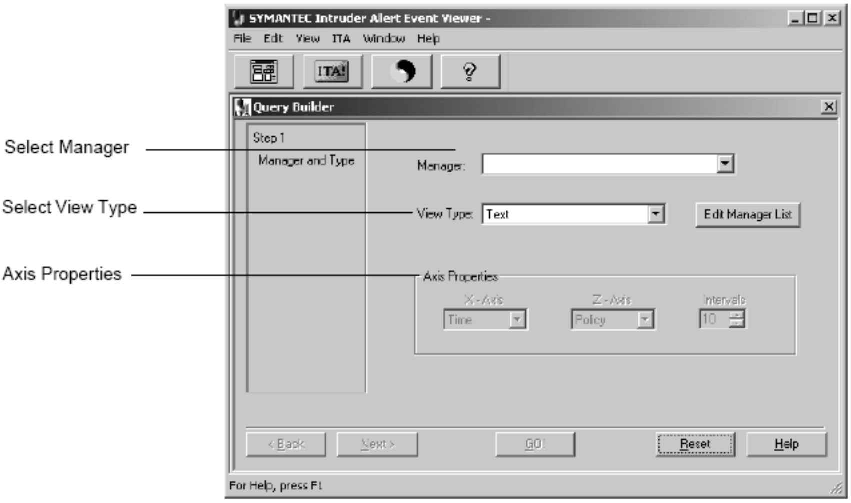
Defining a query

Defining a new query in the Intruder Alert Event Viewer is a three step process involving the three screens of the Query Builder wizard.

Screen one

The following graphic illustrates the first of three screens contained in the Query Builder wizard. In this screen you will select a Manager and a report view type.

Figure 2-20 Query Builder screen one



Manager:

View Type: Text

X-Axis Time

Z-Axis Policy

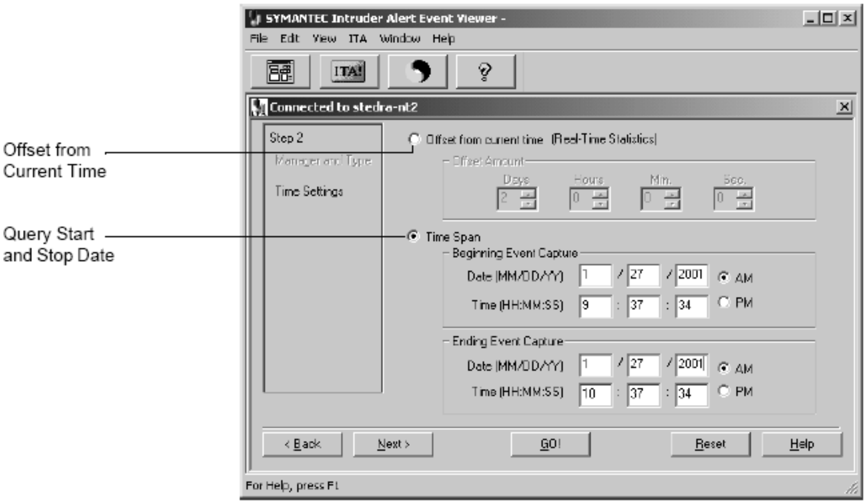
Intervals 10

Note: Several options are available in the Axis Properties box depending on the type of report view that you have chosen. These allow you to define the display parameters for your report.

Screen two

The following graphic illustrates the second of three screens contained in the Query Builder wizard. In this screen you define an effective time or time span.

Figure 2-21 Query Builder screen two


Offset from Current Time
Query Start and Stop Date
SYMANTEC Intruder Alert Event Viewer -
File Edit View ITA Window Help
ITA!
?
Connected to stedra-nt2
< Back
Next >
GO!
Reset
Help

Step 2
Manager and Type
Time Settings

○ Offset from current time (Real-Time Statistics)

Offset Amount: Days 2, Hours 0, Min. 0, Sec. 0

● Time Span

Beginning Event Capture
Date (MM/DD/YY) 1 / 27 / 2001 ● AM
Time (HH:MM:SS) 9 : 37 : 34 ○ PM

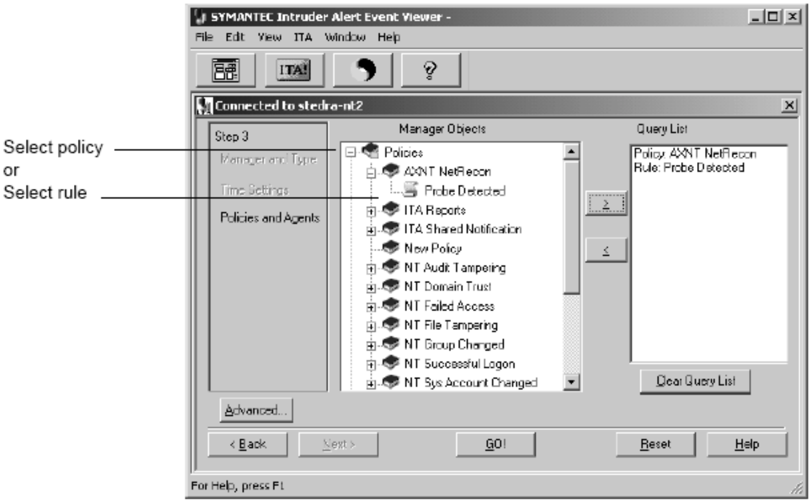
Ending Event Capture
Date (MM/DD/YY) 1 / 27 / 2001 ● AM
Time (HH:MM:SS) 10 : 37 : 34 ○ PM

For Help, press F1

Screen three

In the third screen of the wizard, you specify policies and Agents.

Figure 2-22 Query Builder screen three



Step 3
Manager and Type
Time Settings
Policies and Agents

Manager Objects:
- Policies
  - AXNT NetRecon
    - Probe Detected
  - ITA Reports
  - ITA Shared Notification
  - New Policy
  - NT Audit Tampering
  - NT Domain Trust
  - NT Failed Access
  - NT File Tampering
  - NT Group Changed
  - NT Successful Logon
  - NT Sys Account Changed

Query List:
Policy: AXNT NetRecon
Rule: Probe Detected

For Help, press F1

You may click GO! to run the query and access the report, or you may choose to save the query for later. If you save the query, you may choose from two different formats (.ivw and .ivg).

See "Loading a predefined view" on page 187.

View types

Once a query and view have been defined in the Intruder Alert Event Viewer window, you can click GO! to launch the query. Any information obtained by Event Viewer will be displayed in a preselected format.

The Intruder Alert Event Viewer offers five different view types from which to choose.

- Bar chart
- Line graph
- Pie chart
- Report
- Text

Several options are available in the Axis Properties box, depending on the type of report view you choose. These allow you to define the display parameters for your report.

Note: The pie chart and other graphic views available in the Intruder Alert Event Viewer may display with multicolored shading to the side of the graphic. This is a Crystal Reports issue, and is easily overcome by setting the monitor to a higher resolution or changing the color setting to display true color.

Modifying a graphic view

In the Event Viewer it is possible to right-click on the graphic and select a tool from the graph edit menu to modify the chart view.

See "Modifying a chart view" on page 188.

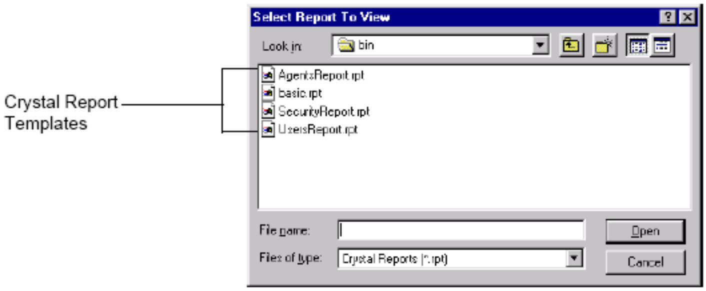
Report view

The report and text views provide more in-depth information about the security events. The details of the security event are clearly visible in the report view. The first page is a summary of the query which was used to generate the report, while subsequent report pages contain the detailed summaries of the security events that occurred during the period specified in the report query.

Report options:

- The basic reports may be customized to present a certain level of detail for specific audiences.
- The data may be presented in a predefined Crystal Reports format.
- Several Crystal Reports formats are included with Intruder Alert at the time of installation.

Figure 2-23 Crystal Report templates



In order to take full advantage of the Crystal Reports capabilities in Intruder Alert, including the option to customize your report page with custom logos, you must own a fully licensed version of Crystal Reports.

Crystal Reports integration with Intruder Alert provides you with the following benefits:

- Choice of a variety of report types
  Choose from sub-reports, conditional reports, summary reports, cross-tabs, form reports, drill-down, OLAP, Top N, multiple detail reports, mailing labels and more.
- Easy access to Intruder Alert event logs
  Connect to over 30 different types of OLAP, SQL, and PC databases including Microsoft SQL Server, Lotus Domino, and Oracle, using supported native ODBC connectivity.
- Ability to customize the look of your report
  Address complex reporting requirements with advanced features including grouping, sorting, sub-reports, and cross-tabs.

To learn more about Crystal Reports visit the following Web site:

http://www.businessobjects.com/

Text view

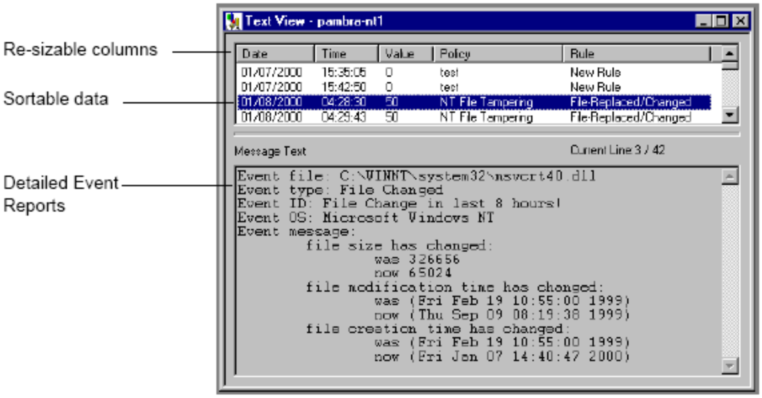
Details of the security event are made available in the text view. Clicking on an event entry will reveal a detailed report about the event.

Text view options:

- Click or double-click on a column header to sort all the information in either ascending or descending order.
- Resize or hide columns by dragging the borders of the column heads with a click-and-hold of the left mouse button.

Below is an example of the alert text view.

Figure 2-24 Text view



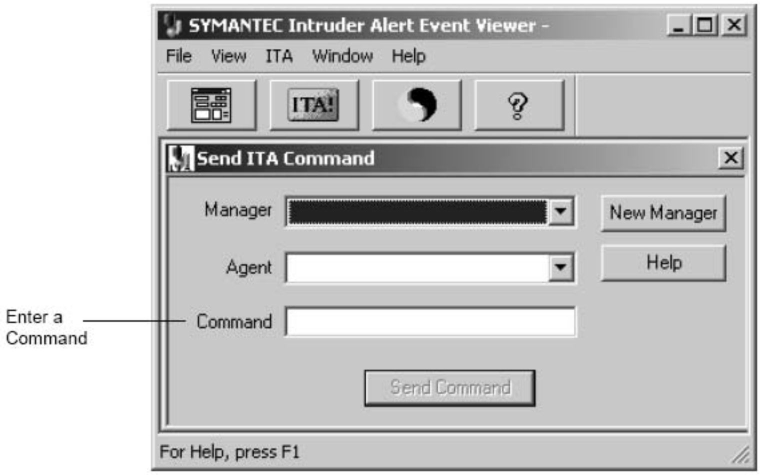
Date	Time	Value	Policy	Rule
01/07/2000	15:35:05	0	test	New Rule
01/07/2000	15:42:50	0	test	New Rule
01/08/2000	04:28:30	50	NT File Tampering	File-Replaced/Changed
01/08/2000	04:29:43	50	NT File Tampering	File-Replaced/Changed

```
Event file: C:\WINNT\system32\msvcrt40.dll
Event type: File Changed
Event ID: File Change in last 8 hours!
Event OS: Microsoft Windows NT
Event message:
          file size has changed:
                    was 326656
                    now 65024
          file modification time has changed:
                    was (Fri Feb 19 10:55:00 1999)
                    now (Thu Sep 09 08:19:38 1999)
          file creation time has changed:
                    was (Fri Feb 19 10:55:00 1999)
                    now (Fri Jan 07 14:40:47 2000)
```

Sending Intruder Alert commands

In the Intruder Alert Event Viewer you can send an Intruder Alert command. Intruder Alert commands are user-defined.

Figure 2-25 Send Intruder Alert command



See “ITA Command criteria” on page 97.

See “Sending an Intruder Alert command to an Agent” on page 191.

Managers and Agents

Intruder Alert Managers and Agents are UNIX daemons or Windows services and do not require a user interface.

Section 2

Administering security

This section discusses the following:

- Chapter 3: Post-installation options
- Chapter 4: Administering Intruder Alert
- Chapter 5: Managing Agents

Chapter 3

Post-installation options

This chapter includes the following topics:

- Post-installation options on UNIX
- Post-installation options on Windows

Note: The instructions in this chapter pertain to immediate post-installation options only. Information regarding connecting Managers and Agents, starting and stopping Managers and Agents, and performing additional administrative tasks using Intruder Alert Administrator, is discussed later in the guide.

Post-installation options on UNIX

This section contains instructions for performing each UNIX post-installation option. UNIX post-installation options include:

- Starting the Manager and Agent
- Stopping the Manager and Agent
- Registering an Agent with additional Managers
- Unregistering an Agent from a Manager
- Changing the Agent label
- Updating NIS Master information on the Agent
- Exiting the post-installation procedure

Starting the Manager and Agent

The start option starts whatever Intruder Alert components reside on that system. If the Manager and Agent reside on the same system, both will be started. If only the Agent resides on that system, only the Agent will be started.

To start the Manager and/or Agent

1. Change to the Intruder Alert bin directory. Type the following command and then press **Enter**:

   ```
   cd /axent/ita/bin
   ```

2. Type the following command and then press **Enter**:

   ```
   ./itarc start
   ```

Stopping the Manager and Agent

The stop option stops whatever Intruder Alert components reside on that system. If the Manager and Agent reside on the same system, both will be stopped. If only the Agent resides on that system, only the Agent will be stopped.

To stop the Manager and/or Agent

1. Change to the Intruder Alert bin directory. Type the following command and then press **Enter**:

   ```
   cd /axent/ita/bin
   ```

2. Type the following command and then press **Enter**:

   ```
   ./itarc stop
   ```

Registering an Agent with additional Managers

If desired, Agents can be registered with multiple Managers. The following instructions describe how to register an Agent with an additional Manager.

To register an Agent with additional Managers

1. Change to the Intruder Alert setup directory. Type the following command and then press **Enter**:

   ```
   cd /axent/ita/bin/<platform_type>
   ```

   where platform_type indicates the type of computer you are using.

2. Start Intruder Alert setup. Type the following command and then press **Enter**:

   ```
   ./itasetup
   ```

3. When prompted with the Intruder Alert setup options, type **2** and then press **Enter** to display the post-installation options.

4. Type **4** and then press **Enter** to register the Agent with an additional Manager.
5. At the Intruder Alert Manager prompt, type the IP address or name of the Manager and then press **Enter**.
6. At the TCP port or service name prompt, do one of the following:
   - To use the default Manager port number of 5051, press **Enter** (recommended).
   - To specify a different TCP port, type the port number or service name and then press **Enter**.

     To use a service name, first associate it with a specific port.
7. At the Authorized Administrator Name prompt, type the username for the administrator and then press **Enter**.
8. At the Manager Password prompt, type the administrator password and then press **Enter**.

   The Agent attempts to register with the specified Manager. If the attempt was successful, a message will appear indicating the registration was complete. If the attempt was unsuccessful, be sure you can ping the Manager's system and then repeat these instructions avoiding any typographical errors.

Unregistering an Agent from a Manager

To unregister an Agent from a Manager

1. Change to the Intruder Alert setup directory. Type the following command and then press **Enter**:

   ```
   cd /axent/ita/bin/<platform_type>
   ```

   where platform_type indicates the type of computer you are using.
2. Start Intruder Alert setup. Type the following command and then press **Enter**:

   ```
   ./itasetup
   ```
3. When prompted with the Intruder Alert setup options, type **2** and then press **Enter** to display the post-installation options.
4. Type **3** and then press **Enter** to unregister the Agent with a Manager.
5. Do one of the following:
   - To unregister from the default Manager indicated in square brackets, press **Enter**.
   - To unregister from one or more other Managers, type the name of each Manager separated by a space and then press **Enter**.

For example, to unregister from the Managers “global” and “enterprise,” type the following at the command prompt and then press **Enter**:

```
global enterprise
```

Changing the Agent label

The Agent label is the name that is used to identify the Agent.

To change the Agent label

1. Change to the Intruder Alert setup directory. Type the following command and then press **Enter**:

   ```
   cd /axent/ita/bin/<platform_type>
   ```

   where platform_type indicates the type of computer you are using.

2. Start Intruder Alert setup. Type the following command and then press **Enter**:

   ```
   ./itasetup
   ```

3. When prompted with the Intruder Alert setup options, type **2** and then press **Enter** to display the post-installation options.
4. Type **5** and then press **Enter** to change the Agent label.
5. The post-installation software displays a numbered list of possible choices for the Agent label. At the prompt, type the number for your choice and then press **Enter**.
6. If you chose to enter a custom label for this agent, type it in at the prompt and then press **Enter**.
7. At the confirmation prompt, do one of the following:
   - To confirm the choice, press **Enter**.
   - To reject the choice and display the list again, type **n** and then press **Enter**.

Updating NIS Master information on the Agent

To update NIS Master information on the Agent

1. Change to the Intruder Alert setup directory. Type the following command and then press **Enter**:

   ```
   cd /axent/ita/bin/<platform_type>
   ```

   where platform_type indicates the type of computer you are using.

2. Start Intruder Alert setup. Type the following command and then press **Enter**:

```
./itasetup
```

3 When prompted with the Intruder Alert setup options, type **2** and then press **Enter** to display the post-installation options.

4 Type **6** and then press **Enter** to change the NIS Master information.

5 At the NIS Master prompt, do one of the following:

- If the Agent will not be an NIS master or slave master, press **Enter**.
- If the Agent will be an NIS master or slave master, type **y** and then press **Enter**.
  Answer the questions that are displayed.

Exiting the post-installation procedure

To exit the post-installation procedure

◆ When the post-installation procedure option list is displayed, type **7** and then press **Enter** to quit the procedure.

Post-installation options on Windows

This section contains instructions for performing each Windows post-installation option. Post-installation options include:

- Starting ITA Manager-Agent Setup
- Stopping or starting the Agent
- Stopping or starting the Manager
- Registering the Agent with additional Managers
- Registering the Agent with additional Managers
- Configuring Agent service properties

Starting ITA Manager-Agent Setup

To start Intruder Alert Setup

◆ From the Windows Start menu, click **Programs > Symantec > Intruder Alert > ITA Mgr-Agt Setup**.
If the Intruder Alert programs were placed in another program group, access ITA Mgr-Agt Setup from that group.
The Manager-Agent Setup dialog box appears.

Stopping or starting the Agent

To stop or start the Agent

1. Start ITA Mgr-Agt Setup.
   See "Starting ITA Manager-Agent Setup" on page 59.
2. In the Manager-Agent Setup dialog box, if the Agent is running and you want to stop it, click **Stop Local Agent**.
3. If the Agent is stopped and you want to start it, click **Start Local Agent**.

Stopping or starting the Manager

To stop or start the Manager

1. Start ITA Mgr-Agt Setup.
   See "Starting ITA Manager-Agent Setup" on page 59.
2. In the Manager-Agent Setup dialog box, if the Manager is running and you want to stop it, click **Stop Local Manager**.
3. If the Manager is stopped and you want to start it, click **Start Local Manager**.

Registering the Agent with additional Managers

To register the Agent with additional Managers

1. Start ITA Mgr-Agt Setup.
   See "Starting ITA Manager-Agent Setup" on page 59.
2. Click **Register to new Manager**.
3. In the Register Local Agent to Manager dialog box, in the Manager field, type the Manager's name.
4. In the Username field, type the Manager's username.
5. In the Password field, type the Manager's password.
6. Under Protocol, do one of the following to select the protocol:
   - Click **TCP/IP**
   - Click **IPX/SPX**
7. Click **OK**.
8. Repeat Steps 3-7 for each Manager.
   The Agent is registered with the listed Managers.

Note: The user attempting to register the Agent with a Manager must have "Register New Agent" privileges to register new Agents. User privileges are managed in Intruder Alert Administrator's User Manager.

Unregistering an Agent from a Manager

Use the Intruder Alert Administrator to unregister an Agent from a Manager.

To unregister an Agent from a Manager

1. In the Administrator tree, expand **Managers**.
   The Managers branch displays all Managers connected to the Intruder Alert Administrator.
   See "Connecting to a Manager" on page 64.
2. Expand the branch of the Manager to which the Agent is registered.
3. In the Registered Agents branch, right-click the Agent and then click **Unregister from Manager** in the drop-down list.
4. In the confirmation dialog box, click **Yes**.

Although the recommended method of unregistering an Agent is through the Intruder Alert Administrator, it may be necessary to force the unregistration process of an Agent from a Manager.

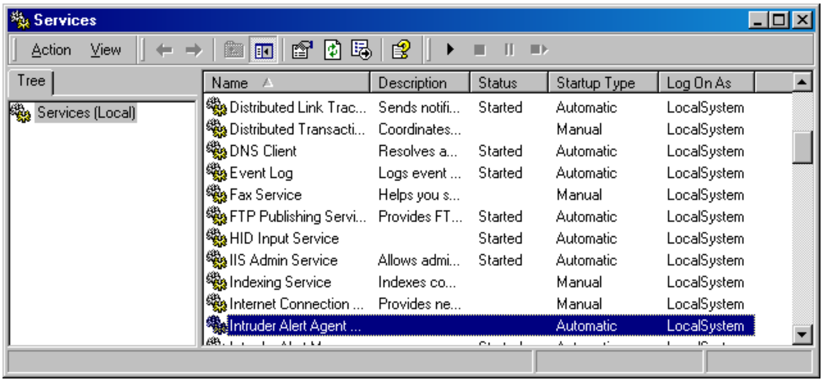
To force unregistration of the Agent from a Manager

1. Start ITA Mgr-Agt Setup.
   See "Starting ITA Manager-Agent Setup" on page 59.
2. In the Manager-Agent Setup dialog box, in the Agent Registration box, click the desired Manager and then click **Unregister**.
   A dialog box appears warning you that this option should only be used if the Agent cannot be unregistered using the Intruder Alert Administrator.
3. In the warning dialog box, click **OK**.
4. Repeat step 2 for each Manager that you want to unregister.
5. When finished, click **OK**.
   The Agent is unregistered from the selected Managers.

Configuring Agent service properties

From the Windows Services window, you can configure the Intruder Alert Agent service properties to automatically start the Agent at system boot time. You can also start, stop, and restart the Agent from the Windows Services window by right-clicking the Agent and selecting the desired action in the drop-down list.

Figure 3-1 Windows Services window



Name	Description	Status	Startup Type	Log On As
Distributed Link Trac...	Sends notifi...	Started	Automatic	LocalSystem
Distributed Transacti...	Coordinates...		Manual	LocalSystem
DNS Client	Resolves a...	Started	Automatic	LocalSystem
Event Log	Logs event ...	Started	Automatic	LocalSystem
Fax Service	Helps you s...		Manual	LocalSystem
FTP Publishing Servi...	Provides FT...	Started	Automatic	LocalSystem
HID Input Service		Started	Automatic	LocalSystem
IIS Admin Service	Allows admi...	Started	Automatic	LocalSystem
Indexing Service	Indexes co...		Manual	LocalSystem
Internet Connection ...	Provides ne...		Manual	LocalSystem
Intruder Alert Agent ...			Automatic	LocalSystem

To configure the Agent service properties

1. In the Windows Control Panel, open Services.
2. In the Windows Services window, double-click Intruder Alert Agent v3.6.1 to launch the Agent Properties dialog box.
3. In the Agent Properties dialog box, in the Startup type text box, select **Automatic** in the drop-down list to ensure that Intruder Alert protection is available at all times.

Chapter 4

Administering Intruder Alert

This chapter includes the following topics:

Starting Intruder Alert Administrator

Intruder Alert Administrator runs only on Windows.

To start Intruder Alert Administrator

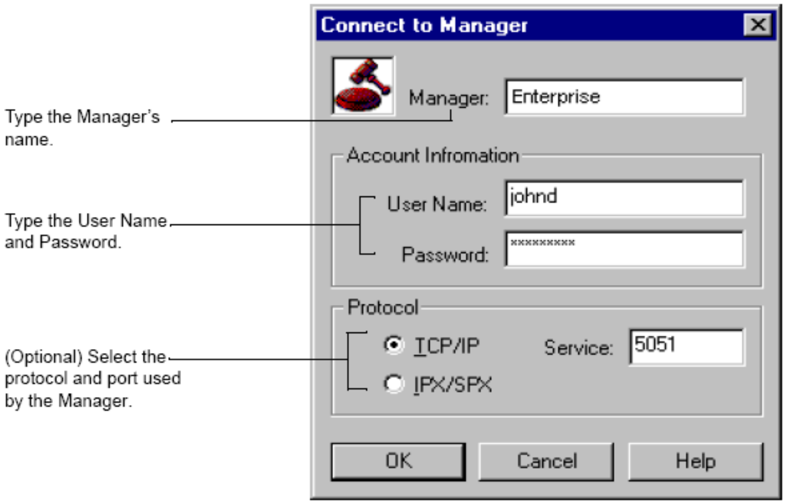
◆ Do one of the following:

- Click the Windows Start menu, and click **Programs > Symantec > Intruder Alert > ITA Administrator**.
- Double-click the application icon on the Windows desktop.

Connecting to a Manager

To connect to a Manager from the Administrator, follow the procedure below, and refer to Figure 4-1.

Figure 4-1 Connect to Manager dialog box



Manager: Enterprise

User Name: johnd

Password: **********

● TCP/IP

○ IPX/SPX

Service: 5051

Type the Manager's name.

Type the User Name and Password.

(Optional) Select the protocol and port used by the Manager.

To connect to a Manager

1 In the Administrator window, in the Intruder Alert tree, click **Managers**.

2 Do one of the following:

- On the toolbar, click **Connect**.
- In the tree, expand **Managers** and then right-click the Manager that you want to connect to. In the drop-down list, click **Connect to Manager**.
- In the tree, right-click **Managers** and then click **Connect to Manager** in the drop-down list.

3 In the Connect to Manager dialog box, in the Manager text box, type the name of the Manager.

4 In the User Name text box, type the Manager username.

5 In the Password text box, type the Manager password.

6 Under Protocol, do one of the following, according to the Manager configuration:

- Click **TCP/IP**
- Click **IPX/SPX**

7 If the Manager is configured to communicate using a port number other than 5051, enter that port number in the Service text box.

The Service text box specifies the port number on the Manager system. The default port number is 5051.

8 Click **OK**.

Intruder Alert Administrator attempts to connect to the Manager. If the connection is successful, the expansion box appears next to the name underneath the Managers branch. If the connection is not successful, an error message will appear.

Intruder Alert supports Manager “reconnects” to unavailable Agents. The Manager will periodically retry any failed attempts to connect to an Agent.

If the attempt to connect fails, repeat the process watching for typographical errors. For example, passwords are case sensitive. Also, verify that you are able to perform a successful nslookup on the Manager system to confirm that the Domain Name Service (DNS) server can resolve the hostname to its IP address. If the Manager will not connect, make sure the Manager daemon or service is running.

Disconnecting from a Manager

To disconnect the Administrator from a Manager, follow the procedure below.

To disconnect from a Manager

1. In the Intruder Alert tree, expand **Managers**.
2. Right-click the Manager and then click **Disconnect from Manager** in the drop-down list.
3. In the Administrator dialog box, click **Yes**.

Deleting a Manager from the Intruder Alert tree

To delete a Manager from the Intruder Alert tree in the Administrator, follow the procedure below.

To delete a Manager from the Intruder Alert tree

1. In the Intruder Alert tree, right-click the Manager and then click **Delete** in the drop-down list.
2. In the Delete dialog box, click **Yes**.

Starting and stopping Managers/Agents

The following instructions describe how to start and stop Managers and Agents manually for each operating system.

Note: If the Manager and Agent reside on the same machine, Intruder Alert starts both the Manager and Agent automatically during system startup.

Starting and stopping a UNIX Manager /Agent

To start and stop a UNIX Manager/Agent

1 At the UNIX prompt, type the command:

```
cd /axent/ita/bin
```

2 Type one of the following commands and then press **Enter**:

Table 4-1 UNIX commands

To	Enter
Stop the Manager and Agent	./itarc stop
Start the Manager and Agent	./itarc start
Stop the Manager only	./itarc stopMgr
Stop the Agent only	./itarc stopAgt

Starting and stopping a Windows Manager/Agent

You can stop and start Intruder Alert components from the Windows command prompt, from the Windows Start menu, or via the Services utility located in the Control Panel.

To start and stop a Windows Manager/Agent from the Windows command prompt

1 At the Windows command prompt, go to the following directory: <system disk>:\Program Files\Symantec\ITA\bin\

2 Enter one of the following commands:

Table 4-2 Windows commands

To	Enter
Stop the Manager	mgrnt stop

Table 4-2 Windows commands

To	Enter
Start the Manager	mgrnt start
Stop the Agent	agtnt stop
Start the Agent	agtnt start

To start and stop a Windows Manager/Agent from the Windows Start menu

1. Click **Start > Programs > Symantec > Intruder Alert > ITA Mgr-Agt Setup**.
   The Manager-Agent Setup dialog box appears.
2. To stop the Agent, click **Stop Agent**.
3. To stop the Manager, click **Stop Manager**.

To start and stop the Windows Manager/Agent with the Windows service utility

1. Under the Windows Control Panel, open Services.
2. In the Services window, do one of the following:
   - Right-click Intruder Alert Agent v3.6.1
   - Right-click Intruder Alert Manager v3.6.1
3. To stop the Manager or Agent, click **Stop** in the drop-down list.
4. To start the Manager or Agent, click **Start** in the drop-down list.
   The Status column indicates whether the service is stopped or started.

Note: Intruder Alert Agent services should be configured so that Startup Type is Automatic, so that protection can be started at boot time.
See "Configuring Agent service properties" on page 61.

Managing user accounts and privileges

The User Manager controls who can access the Intruder Alert Administrator and Intruder Alert Event Viewer, and what privileges they have when installing and administering it. The following table lists the privileges that can be assigned to a user.

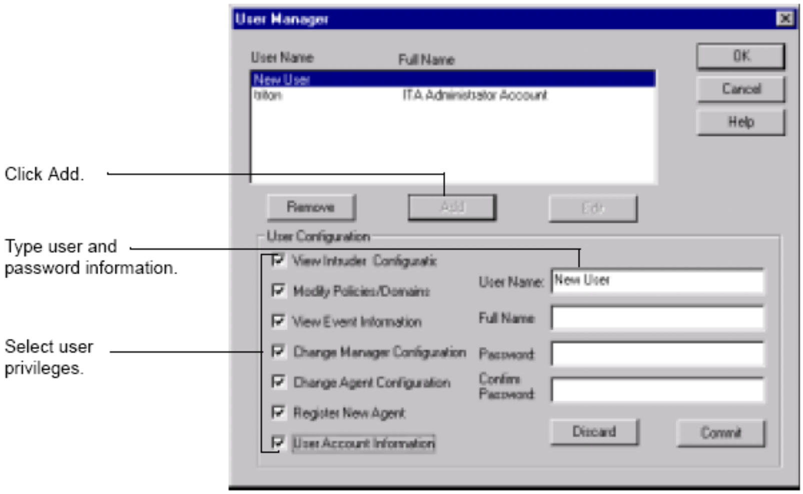
Table 4-3 User privileges

Privilege	Description
View Configuration	Allows the user to view configuration information
Modify Policies/Domains	Allows the user to organize domains and apply/ remove policies
View Event Information	Allows the user to view event information
Change Manager Configuration	Not applicable
Change Agent Configuration	Allows the user to configure email, paging, and the Agent to monitor additional external audit logs Note: The View Configuration privilege must be checked
Register New Agent	Allows the user to register an Agent to a Manager or additional Managers
User Account Information	Allows the user to add new users and define user privileges

Creating a new user account

Refer to Figure 4-2 when creating a new user account.

Figure 4-2 User Manager window



Click Add.

Type user and password information.

Select user privileges.

User Name	Full Name
New User	
triton	ITA Administrator Account

User Configuration

☑ View Intruder Configuratic
☑ Modify Policies/Domains
☑ View Event Information
☑ Change Manager Configuration
☑ Change Agent Configuration
☑ Register New Agent
☑ User Account Information

User Name: New User
Full Name:
Password:
Confirm Password:

To create a new user account

1. In the Intruder Alert tree, click the Manager to select it.
2. Do one of the following:
   - In the menu bar, click **Manager > Security > User Manager**.
   - In the Intruder Alert tree, right-click the Manager and then click **User Manager** in the drop-down list.
3. In the User Manager window, click **Add**.
4. Under User Configuration, assign privileges to the new user by selecting the check box for that privilege.
5. In the User Name text box, type a username for the new user.
6. In the Full Name text box, type the user's full name.
7. In the Password text box, type the password for the new user.
8. In the Confirm Password text box, retype the password.
9. Click **Commit**.
10. When finished, click **OK**.
    The new user is added with the specified privileges.

Modifying user privileges

User privileges can be changed after the user account has been created. In order to change account information, you must have User Account Information privileges.

To modify user privileges

1. In the Intruder Alert tree, right-click the desired Manager and then click **User Manager** in the drop-down list.
2. In the User Manager window, in the User Name text box, select the user and then click **Edit**.
3. Make the desired modifications and then click **Commit**.
4. When finished, click **OK**.
   User Manager changes the user's privileges.

Changing user passwords

To maintain security and protect the use of Intruder Alert, the administrator should periodically change user passwords. In order to change account information, you must have User Account Information privileges.

Note: If an Admin/User account was used during installation to register the Agents with the Manager, communication between the Agent and Manager will disconnect if the password is changed.

To change user passwords

1. In the Intruder Alert tree, right-click the desired Manager and then click **User Manager** in the drop-down list.
2. In the User Manager window, in the User Name text box, select the user and then click **Edit**.
3. In the Password text box, type the new password.
4. In the Confirm Password text box, retype the new password and then click **Commit**.
5. When finished, click **OK**.
   The User Manager changes the user's password.

Removing a user account

A Security Administrator may use a generic user account to register Agents to Managers. If this account is subsequently deleted or the password is changed, all communications between the Agents and Managers that were established using the account will be broken.

Symantec recommends that you do not use a temporary user account to set up Agent/Manager communication. If you do use such an account, make it a generic account, ensure that it is limited to trusted users only and do not delete it.

To remove a user account

1. In the Administrator window, in the tree, right-click the Manager and then click **User Manager** in the drop-down list.
2. In the User Manager window, in the User Name text box, select the user.
3. Click **Remove**.
4. Click **OK**.

General administrative tasks

The following tasks are discussed in this section:

- Printing tree view information

- Deleting a folder
- Using online help

Printing tree view information

Intruder Alert Administrator allows you to select an object in the Intruder Alert tree, and print information about that object and all objects beneath it.

To print tree view information

1. Connect to a Manager.
2. In the Intruder Alert tree, click the desired object.
3. On the menu bar, click **File > Print**.
4. In the Print dialog box, click **OK**.
   Information about the object is sent to the printer.

To print tree view information to a file

1. Connect to a Manager.
2. In the Intruder Alert tree, click the desired object.
3. On the menu bar, click **File > Print To File**.
4. In the Print to File dialog box, specify the destination folder and filename.
5. Click **OK**.
   The information is saved in the specified file.

Deleting a folder

The following instructions describe the process for deleting a folder item in the Intruder Alert tree. Branches created by Intruder Alert Administrator during installation (e.g., Managers, Policies, Registered Agents, etc.) cannot be deleted.

To delete a folder

1. In Intruder Alert Administrator, do one of the following:
   - In the tree, click the folder, and then in the toolbar, click **Delete**.
   - In the tree, right-click the folder and then click **Delete** in the drop-down list.
2. Click **Yes** to confirm the deletion.

Using online help

To use online help

1. On the menu bar, click **Help > Contents & Index**.

   Help topics can be located in one of three ways:

   - Contents
   - Index
   - Find

2. When the Help Topics dialog box appears, to select the desired search method, do one of the following:

   - Click **Contents**
   - Click **Index**
   - Click **Find**

Table 4-4 Online help search methods

Search method	Description
Contents	A hierarchical listing of topics organized in a table of contents.
Index	A list of indexed words or phrases designed to help find topics in the online help.
Find	A tool that searches for any word or combination of words found in the online help.

Using the single.exe command on Windows

You can use the single.exe command on the Windows command line to register and unregister local Agents to a Manager. The command also provides options to list all Managers to which a local Agent is registered, and to print out the usage information for the command itself.

The single.exe command resides in the folder:

<system disk>:\Program Files\Symantec\ITA\bin\

The complete syntax for single.exe is:

```
single.exe [-h] [-l] [-r:<manager>:<user>:<password>:<port>]
[-u:<manager>]
```

where the angle bracketed (<>) arguments are replaced by your actual manager name or IP address, username, password, and port number, and where the options are as follows:

-h	Print this usage message.
-l	List all the Managers to which the local Agent is registered.
-r	Register the local Agent to a Manager using the provided values.
-u	Unregister the local Agent from a Manager.

Use of the single.exe command is detailed in the following sections:

See “Registering an Agent on Windows” on page 79.

See “Unregistering an Agent from a Manager” on page 80.

See “Determining Agent registration information” on page 82.

Using the itasetup command on UNIX

You can use the itasetup command on UNIX to do various tasks, including registering and unregistering local Agents to a Manager. The command also provides options to list all Managers to which a local Agent is registered, to stop Agent or Manager processes, and to print out the usage information for the command itself.

The itasetup command resides in the folder:

/axent/ita/bin/<platform type>/

The complete syntax for itasetup is:

```
itasetup [-h] [-d] [-a] [-m] [-l]
[-r:<manager>:<user>:<password>:<port>] [-u:<manager>]
```

where the angle bracketed (<>) arguments are replaced by your actual manager name or IP address, username, password, and port number, and where the options are as follows:

-h	Print this usage message.
-d	Verbose output.
-a	Stop the Agent process.
-m	Stop the Manager process.
-l	List all the Managers to which the local Agent is registered.
-r	Register the local Agent to a Manager using the provided values.

-u	Unregister the local Agent from a Manager.

Use of itasetup command line options is detailed in the following sections:

See “Registering an Agent on UNIX” on page 77.

See “Unregistering an Agent from a Manager” on page 80.

See “Determining Agent registration information” on page 82.

Chapter 5

Managing Agents

This chapter includes the following topics:

Creating and deleting a domain

In Intruder Alert, Agents are grouped in domains, and policies are applied to all Agents in the domain. Domains are organized according to common criteria such as operating system, location, or workgroup.

Creating a domain

To create a domain

1. In Intruder Alert Administrator, connect to a Manager, and expand the Manager's branch.
2. In the Intruder Alert tree, right-click **Domains** and then click **New** in the drop-down list.
   The new domain appears in the Intruder Alert tree as New Domain.
3. In the right pane, in the Label text box, type a name for the new domain.
4. Optionally, in the Description text box, type a description of the domain.
5. In the tree, click **New Domain** to update the name.

The new domain is created. Your next steps are to add Agents and apply policies to the new domain.

See "Adding an Agent to a domain" on page 76.

See "Applying policies to a domain" on page 127.

Deleting a domain

When you delete a domain, Agents belonging to that domain are still registered to the Manager, and policies continue to reside in the Policies branch on the Manager.

To delete a domain

1. In the tree, right-click the domain and then click **Delete** in the drop-down list.
2. In the dialog box, click **Yes** to confirm the deletion.

Adding an Agent to a domain

To add an Agent to a domain

1. In the tree, expand **Managers** and then expand the desired Manager.
   See "Connecting to a Manager" on page 64.
2. In the Registered Agents branch, right-click the Agent and then click **Add to Domain** in the drop-down list.
3. In the Add <Agent> to Domain dialog box, select the desired domain and then click **OK**.
4. For multiple domains, do one of the following:
   - Press **Shift** and select the first and last of a group of desired domains, and then click **OK**.
   - Press **Ctrl** and select each desired domain, and then click **OK**.

   The Agent is added to each selected domain.

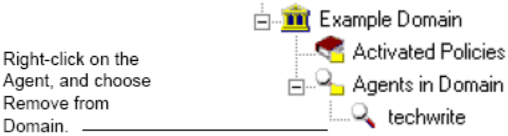
Removing an Agent from a domain

To remove an Agent from a domain

1. In the tree, expand **Managers** and then expand the desired Manager.
   See "Connecting to a Manager" on page 64.

2 In the Domains branch, expand the desired domain and then expand **Agents in Domain**.

Figure 5-1 Removing an Agent


Right-click on the Agent, and choose Remove from Domain.

3 Right-click the Agent, and then click **Remove from Domain** in the drop-down list.

4 In the confirmation dialog box, click **Yes**.
The Agent is removed from the selected domain. However, Agent remains registered to the Manager, and still resides in the Registered Agents branch.

Registering an Agent to a Manager

Intruder Alert Agents can be registered to one or more Managers at the same time. The following table lists the corresponding setup utility executable for each supported operating system.

Table 5-1 Setup executables

Operating system	Setup executable
UNIX	itasetup
Windows	single.exe

Note: You cannot register an Agent to a Manager by dragging and dropping from one Manager to another.

Registering an Agent on UNIX

You can register a local Agent to a Manager by using the itasetup utility in one of two modes:

- Interactive
- Command line option

Procedures for both modes are provided in this section.

To register an Agent on UNIX using interactive mode

1. At the system console, type the following command:
   ```
   cd /axent/ita/bin/<platform type>
   ```
   and then press **Enter**.
2. Type the command:
   ```
   ./itasetup
   ```
   and then press **Enter**.
3. When prompted with the Intruder Alert setup options, type:
   ```
   4
   ```
   and then press **Enter**.
   The post-installation options are listed.
4. To register the Agent with a Manager, type:
   ```
   3
   ```
   and then press **Enter**.
5. At the Manager name prompt, do one of the following:
   - Type the name of the Manager and then press **Enter**.
   - Type the IP address of the Manager and then press **Enter**.
6. At the Manager service port prompt, do one of the following:
   - To accept the default service port of 5051 for the Manager, press **Enter** (recommended).
   - To specify a different service port, type the port number and then press **Enter**.
7. At the user name prompt, type the username for the Manager system and then press **Enter**.
8. At the password prompt, type the password for the Manager and then press **Enter**.
9. At the Agent service port prompt, do one of the following:
   - To accept the default service port for the Agent, press **Enter** (recommended).
   - To specify a different service port for the Agent, type the port number and then press **Enter**.

   The Agent attempts to register with the specified Manager. If the attempt was successful, a message will appear indicating that the registration was complete. If the attempt is unsuccessful, troubleshoot the situation with the following procedure.

To register an Agent on UNIX using command line mode

1. At the system console, type the following command:

```
cd /axent/ita/bin/<platform type>
```

and then press **Enter**.

2 Type the following command and then press **Enter**:

```
itasetup -r:<manager>:<user>:<password>:<port>
```

where the angle bracketed (<>) arguments are replaced by your actual manager name or IP address, username, password, and port number.

To troubleshoot Agent registration on UNIX

1 Verify that the Manager and Agent are running.

2 Make sure the Manager and Agent can ping each other.

3 Verify that the hostnames of both the Manager and the Agent are known by the DNS server, using tools like nslookup.

4 Repeat the registration process being careful to avoid any typographical errors.

Registering an Agent on Windows

You can register an Agent by using ITA Mgr-Agt Setup via the Start menu, or by using single.exe on the Windows command line. Both procedures are provided in this section.

To register an Agent on Windows using ITA Mgr-Agt Setup

1 From the Start menu, click **Programs > Symantec > Intruder Alert > ITA Mgr-Agt Setup**.

2 In the Manager-Agent Setup dialog box, click **Register to new Manager**.

3 In the Register Local Agent to Manager dialog box, in the Manager text box, type the name of the Manager.

4 In the User Name text box, type the user name for the Manager system.

5 In the Password text box, type the password for the Manager.

6 In the Protocol group text box, select the protocol and service number used by the Manager.

7 Click **OK**.
The Manager establishes communication with the Agent.
Intruder Alert supports Manager “reconnects” to unavailable Agents. The Manager will periodically retry any failed attempts to connect to an Agent. If the attempt is unsuccessful, troubleshoot the situation with the following procedure.

To register an Agent using the Windows command line

1. To open a command line window, click **Start > Run**, and in the Run dialog box, type:

   ```
   cmd
   ```

2. In the Run dialog box, click **OK**.

3. To change to the correct directory, type:

   ```
   cd <system disk>:\Program Files\Symantec\ITA\bin\
   ```

   where <system disk> is replaced by the drive letter where your Program Files folder resides.

4. Type the following command and then press **Enter**:

   ```
   single.exe -r:<manager>:<user>:<password>:<port>
   ```

   where the angle bracketed (<>) arguments are replaced by your actual manager name or IP address, username, password, and port number.

To troubleshoot Agent registration on Windows

1. Verify that the Manager and Agent are running.

2. Make sure the Manager and Agent can ping each other.

3. Verify that the hostnames of both the Manager and the Agent are known by the DNS server, using tools like nslookup.

4. Repeat the registration process being careful to avoid any typographical errors.

Unregistering an Agent from a Manager

Unregistering an Agent from a Manager terminates the Manager-Agent relationship—the Agent will no longer report to the Manager. The only way to restore the Manager-Agent relationship is to reregister the Agent with the Manager.

From Intruder Alert Administrator, you can unregister Agents on UNIX or Windows from Managers installed on UNIX or Windows.

You can use single.exe on the Windows command line, or itasetup on UNIX to unregister local Agents from a Manager.

All three procedures are provided in this section.

To unregister an Agent from a Manager using Administrator

1. In Intruder Alert Administrator, connect to the desired Manager.
   See “Connecting to a Manager” on page 64.

2 In the Intruder Alert tree, expand **Managers** and the desired Manager, and then expand **Registered Agents**.
The list of registered Agents should be visible.

3 Right-click the Agent and then click **Unregister from Manager** in the drop-down list.

4 In the Unregister Agent dialog box, click **Yes**.

To unregister a local Agent using single.exe on Windows

1 To open a command line window, click **Start > Run**, and in the Run dialog box, type:

```
cmd
```

2 In the Run dialog box, click **OK**.

3 To change to the correct directory, type:

```
cd <system disk>:\Program Files\Symantec\ITA\bin\
```

where <system disk> is replaced by the drive letter where your Program Files folder resides.

4 Type the following command and then press **Enter**:

```
single.exe -u:<manager>
```

where the <manager> is replaced by your actual manager name or IP address.

To unregister a local Agent using itasetup on UNIX

1 At the system console, type the following command:

```
cd /axent/ita/bin/<platform type>
```

and then press **Enter**.

2 Type the following command and then press **Enter**:

```
itasetup -u:<manager>
```

where <manager> is replaced by your actual manager name or IP address.

Performing Agent management tasks

This section describes the following Agent management tasks:

- Determining Agent registration information
- Renaming an Agent on Windows
- Configuring the Agent for email notification
- Configuring the Agent for pager notification
- Configuring external audit log monitoring

Determining Agent registration information

On either a Windows or a UNIX command line, you can list all the Managers to which an Agent is registered. The commands are:

Windows:	single.exe
UNIX:	itasetup

To list Agent registration information on Windows

1. To open a command line window, click **Start > Run**, and in the Run dialog box, type:
   ```
   cmd
   ```
2. In the Run dialog box, click **OK**.
3. To change to the correct directory, type:
   ```
   cd <system disk>:\Program Files\Symantec\ITA\bin\
   ```
   where <system disk> is replaced by the drive letter where your Program Files folder resides.
4. Type the following:
   ```
   single.exe -l
   ```
   and then press **Enter**.

To list Agent registration information on UNIX

1. At the system console, type the following command:
   ```
   cd /axent/ita/bin/<platform type>
   ```
   and then press **Enter**.
2. Type the following command and then press **Enter**:
   ```
   itasetup -l
   ```

Renaming an Agent on Windows

To rename an Agent on Windows

1. From the Start menu, click **Programs > Symantec > Intruder Alert > ITA Mgr-Agt Setup**.
2. In the Manager-Agent Setup dialog box, click **Edit Label**.
   The Caption text box becomes active.
3. In the Caption text box, rename the Agent as desired.
4. Click **Commit**.

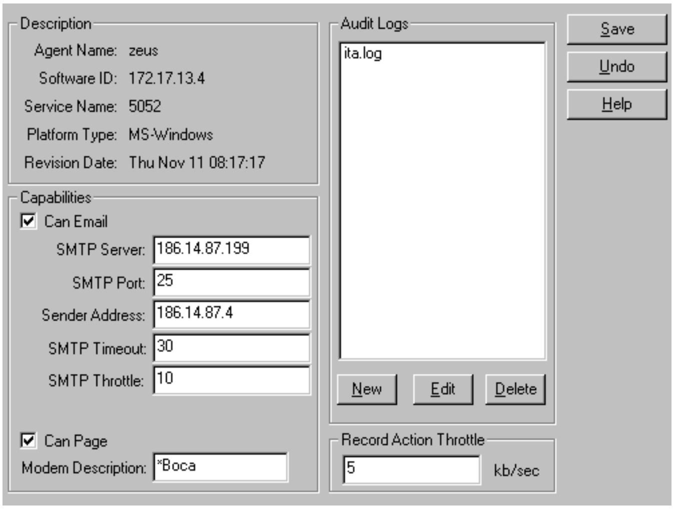
5 Exit the Intruder Alert Mgr-Agt Setup utility by clicking the X in the top right corner of the window.

The Agent's label is changed. You can view the change in Intruder Alert Administrator.

Configuring the Agent for email notification

Before an Agent can send email notification messages, it must be configured to use the SMTP server. The Agent can only send email, not receive it.

Figure 5-2 Agent configuration fields



Description

Agent Name: zeus

Software ID: 172.17.13.4

Service Name: 5052

Platform Type: MS-Windows

Revision Date: Thu Nov 11 08:17:17

Capabilities

☑ Can Email

SMTP Server: 186.14.87.199

SMTP Port: 25

Sender Address: 186.14.87.4

SMTP Timeout: 30

SMTP Throttle: 10

☑ Can Page

Modem Description: *Boca

Audit Logs

ita.log

Record Action Throttle

5 kb/sec

In addition to configuring the Agent, a Send Email action must be added to a policy specifying the email addresses of the people to be notified.

When a Send Email action is executed, the Agent checks to see if it is configured to send email. If it is, it will send the email message. If it cannot, it will send the request to the Manager who will then pass the request to a registered Agent that can send the email.

Note: Symantec recommends that all Agents be configured to send email.

To configure an Agent to send email

1 Configure an SMTP Server in your enterprise.

2 In the Intruder Alert tree, connect to a Manager and expand its branch.

See “Connecting to a Manager” on page 64.

3 Expand **Registered Agents** and then click the desired Agent.

4 In the Agent configuration fields in the right pane, under Capabilities, check **Can Email**.

5 In the SMTP Server text box, type the SMTP server name or IP address.

6 In the SMTP Port text box, if the port configured for email is different than the default, type the port number.

7 In the Sender Address text box, type the sender’s email address.

8 In the SMTP Timeout text box, type the number of seconds before the SMTP server will time out.

9 In the SMTP Throttle text box, optionally modify the default SMTP throttle value.
The SMTP throttle value defines the maximum number of emails that can be sent per minute. This throttle protects the network from excess traffic.

10 Click **Save**.

Configuring the Agent for pager notification

An Intruder Alert Agent can be configured to page a security administrator when an attack has been detected. In addition to configuring the Agent, a Send Page action must be added to a policy specifying the pager number to be dialed and the numeric sequence to be sent.

When a Send Page action is executed, the Agent checks to see if it is configured to page. If it is, it will send the pager notification message. If it cannot, it will send the request to the Manager. The Manager will then pass the request to a registered Agent that can send the page.

Note: Every Agent does not need to be capable of paging. To learn which Agents are capable, click a connected Manager in the Intruder Alert tree and then select Paging from the Manager menu.

To configure an Agent to send a page

1 Install a modem device on the Agent system.

2 In the Intruder Alert tree, in the Registered Agents branch, click the desired Agent.

3 In the Agent configuration fields, check **Can Page**.

4 In the Modem Description text box, type the modem description for the Agent platform. See the guidelines below.

- On UNIX, type:

  `/dev/<port name>`

  For example:

  `/dev/pty9`

Note: Hewlett-Packard recommends HP modems when configuring modem devices under HP-UX. Non-HP modems may cause unpredictable behavior.

- On Windows, type the name of the modem.

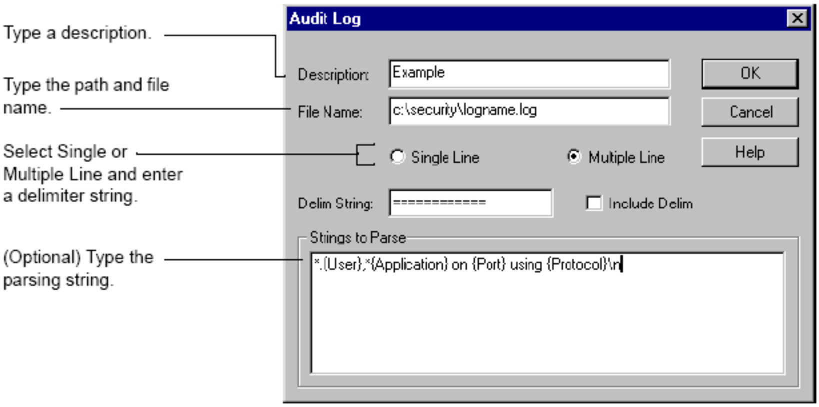
  Check in the Control Panel under Modems to identify the modem or modems available on the Agent system. If the exact name of the modem is not known, type what is known and use an asterisk (*) wildcard operator.

5 Click **Save**.

Configuring external audit log monitoring

Operating systems and applications generate events and store them in log files. Intruder Alert can be configured to monitor these files for security-related events. An external audit log is a log file that Intruder Alert does not automatically monitor.

Figure 5-3 Audit Log dialog box



Type a description.

Type the path and file name.

Select Single or Multiple Line and enter a delimiter string.

(Optional) Type the parsing string.

Description: Example

File Name: c:\security\logname.log

○ Single Line ● Multiple Line

Delim String: ============ □ Include Delim

Strings to Parse

```
*.{User},*{Application} on {Port} using {Protocol}\n
```

Intruder Alert can be configured to parse or extract specific data out of an event message. Parsing makes specific event content more accessible when viewing the event message in Intruder Alert Event Viewer. Events need a record delimiter to separate events. Parsing rules are optional. Define parsing rules for only the desired event types.

See "Operating system collectors" on page 221.

To configure Intruder Alert to monitor an external audit log

1. In the Intruder Alert tree, connect to a Manager and expand its branch.
   See "Connecting to a Manager" on page 64.
2. Expand **Registered Agents** and then click the desired Agent.
3. In the Agent configuration fields in the right pane, under Audit Logs, click **New**.
4. In the Audit Log dialog box, in the Description text box, type a description of the log file.
5. In the File Name text box, type the path and filename of the log file to monitor.
6. Do one of the following:
   - Click **Single Line** for single line log files.
   - Click **Multiple Line**, and, in the Delim String text box, specify a record delimiter for multiple line log files.

   Determine if the log file is a single or multiple line file and what the record delimiter is by opening the log using a text editor, such as Notepad on Windows or vi on UNIX.
7. Optionally click in the Strings to Parse text box, and type the event string or strings to parse.
   Parsing allows you to gather specific information from an event message and use that information for reporting in the Intruder Alert Event Viewer.
   Use the guidelines in the table below for parsing events.

Table 5-2 Parsing guidelines

To	Use
Label parsed fields Intruder Alert captures whatever information appears in braces ({})and stores it for Intruder Alert Event Viewer reporting.	{Name of field} Braces {}, not square brackets [].
Represent spaces	Press the spacebar
Represent hard (carriage) returns	\n
Represent single missing characters	?

Table 5-2 Parsing guidelines

To	Use
Represent multiple missing characters or words	*

Example: The following is an example event message:

```
event: jdoe logged on to Jaguar at 14:05 on 09/18/2001
```

The following parsed string would capture the relevant information contained in that event message.

```
event:{User} {Action} to {System} at {Time} on {Date}
```

8 To parse additional messages, press **Enter** and type the parsed event message.

9 When finished, click **OK**.

Intruder Alert monitors the specified audit log and parses the specified event messages.

Section 3

Securing systems

This section discusses the following:

- Chapter 6: Policies, rules, and criteria
- Chapter 7: Administering policies
- Chapter 8: Creating and modifying policies
- Chapter 9: File and directory security
- Chapter 10: Event context capturing

Policies, rules, and criteria

This chapter includes the following topics:

Policies and rules

Intruder Alert policies describe how to detect specific events and what actions to take once they are identified. When intruders attack a host, they leave a trail of audit log messages. These messages are to information security experts what fingerprints are to criminal investigators.

Policies contain rules; and rules contain criteria. There are three types of criteria: Select, Ignore, and Action.

Policy rules

A rule is a logical statement comprised of up to three parts:

- Select criteria (If)
- Ignore criteria (And)
- Actions (Then)

These criteria relate together to provide functional logic for the policy rule. Select items define selection, while Ignore items define exceptions. Therefore, if the event contains the selection criteria, but does not contain the exception criteria, the rule action will trigger. For example,

If <Select> is true

AND

<Ignore> is not true

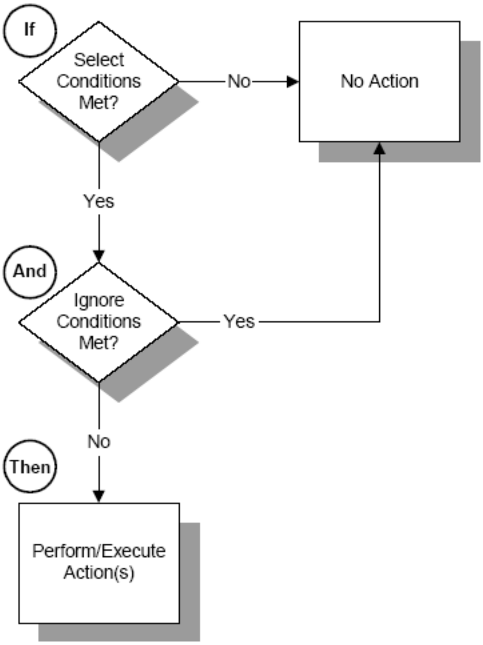
THEN

Perform <Action>

Note: Valid rules typically contain one or more Select criteria, an optional Ignore criteria, and one or more Actions. All criteria do not need to be present for the rule to be valid.

The following graphic illustrates the If-And-Then logic of policy rules.

Figure 6-1 Rule Logic

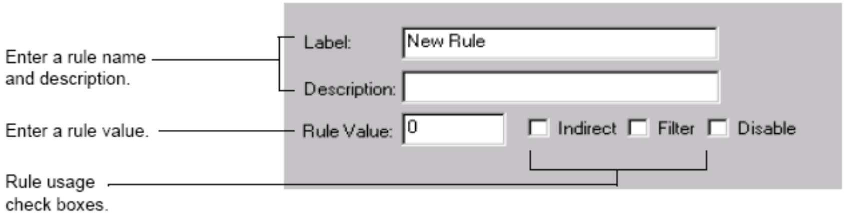


A single policy may contain several rules, and a rule may contain several criteria. While there is no practical limit to the number of criteria contained in a rule, or the number of rules contained in a policy, there is a 64k limit on the size of a policy file, which is roughly 25 rules.

Rule definition

When you create a rule in Intruder Alert, you are presented with the following boxes in the right pane of the Intruder Alert Administrator window.

Figure 6-2 Rule definition fields



Label: New Rule

Description:

Rule Value: 0 □ Indirect □ Filter □ Disable

The first two elements include the Label and Description. The Label text box contains the rule name. Rule names may be up to 31 characters long. The Description text box briefly defines the rule and is limited to 256 characters.

Rule value

The rule value defines severity level of the event. Values range between 0 and 100, with 100 being the most severe. Policies in the product have the following values:

0	Administrative (does not detect system events.)
20	FYI
50	Alert
90	Emergency

The following table is a guide for rule values.

Table 6-1 Rule value and security

Value range	Security level	Security threat
0-33	Low	For Your Information (FYI) Events within this range pose a minimal threat.
34-66	Medium	Alert—Moderate Concern Events within this range pose a moderate threat.
67-100	High	Emergency—Serious Concern Events within this range pose a high threat.

Rule type

Adjacent to the Rule Value field are three check boxes. These check boxes define how the rule functions. The following table defines each option.

Table 6-2 Rule usage

Usage type	Description
Indirect	Indirect rules are referenced within other rules. For example, select criteria could be specified in an indirect rule, and other rules could select or ignore the indirect rule. This makes it possible to centralize select criteria changes for all system messages into one rule.
Filter	If the filter rule criteria are met, all rules in the policy will be ignored. The filter rule contains only select criteria. If the select criteria matches an event, all other rules in the policy are ignored.
Disable	The Disable check box disables the rule. It allows you to retain the rule and its configuration without deleting it.

Select and Ignore criteria

The same criteria exists for both Select and Ignore, with one exception, the Select Timer. There is no Ignore Timer option.

This section provides information about the following:

- System Message criteria
- ITA Status criteria
- ITA Error criteria
- ITA Command criteria
- Flag criteria
- Timer criteria
- Date criteria
- ITA Rule criteria
- User criteria
- System criteria
- Windows Registry Key criteria

System Message criteria

The System Message criteria contains the event text for which to search. System Message criteria can be used to select or ignore an event. If a Select system message matches an event, and does not match an Ignore system message, the actions specified in the rule will trigger.

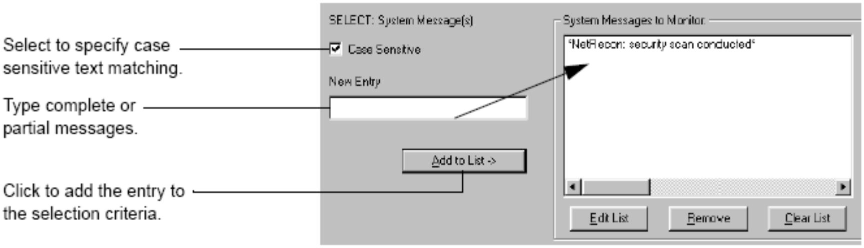
System Message criteria support case sensitive text matching and wildcard operators. Select the check box if you want the event text search to be case sensitive. Use the (*) wildcard operator for multiple characters or words and the (?) wildcard operator for single characters.

Following are examples of text contained in a system message:

- *ftpd connection*
- *Successful login*guest*
- *Failed ?dmin login*

To configure a system message, add the desired search string to the System Messages to Monitor box.

Figure 6-3 System message box



Select to specify case sensitive text matching.

Type complete or partial messages.

Click to add the entry to the selection criteria.

SELECT: System Message(s)

☑ Case Sensitive

New Entry

System Messages to Monitor

NetRecon: security scan conducted

ITA Status criteria

The ITA Status criteria selects or ignores text associated with Intruder Alert status messages. Intruder Alert generates various messages regarding the

Manager's and Agent's status. Intruder Alert Managers and Agents handle all status messages internally.

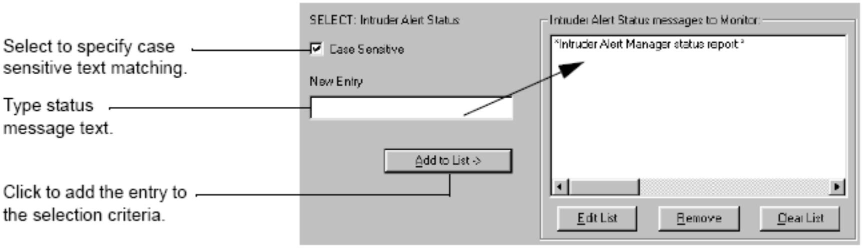
The Status Criteria supports case sensitive text matching and wildcard operators. Select the check box if you want the event text search to be case sensitive. Use an asterisk (*) wildcard operator in place of multiple characters and the question mark (?) wildcard operator in place of single characters.

The following are examples of status messages:

- *ITA manager on ambrosia is updating*
- *Agent configuration modified*
- *ITA agent active datastream report*

To configure an ITA Status criteria, add the desired text in the Intruder Alert Status Messages to Monitor box, as illustrated below.

Figure 6-4 Intruder Alert status criteria



Select to specify case sensitive text matching.

Type status message text.

Click to add the entry to the selection criteria.

SELECT: Intruder Alert Status
☑ Case Sensitive
New Entry
Add to List ->
Intruder Alert Status messages to Monitor:
Edit List
Remove
Clear List

Intruder Alert Manager status report

ITA Error criteria

The ITA Error criteria selects or ignores Intruder Alert error messages. Intruder Alert generates various error messages and logs them in the manager.log or agent.log files located in the directory:

<system disk>:\Program Files\Symantec\ITA\system\<system name>

View the contents of this log file by opening it in a text editor.

Note: The manager.log and agent.log files are created during run time. If no errors have occurred, these files will not exist.

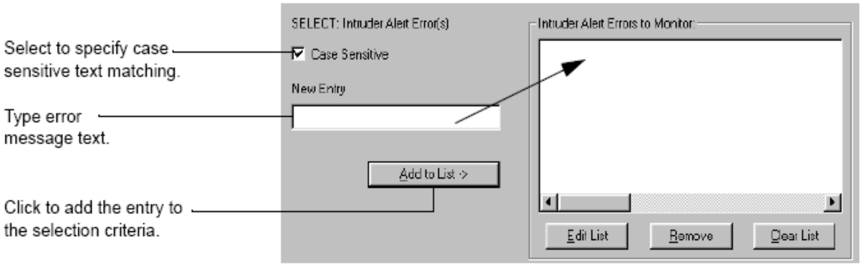
ITA Error criteria supports case sensitive text matching and wildcard operators. Select the check box if you want the event text search to be case sensitive. Use the asterisk (*) wildcard operator in place of multiple characters and the question mark (?) wildcard operator in place of single characters.

The following are examples of ITA Error criteria:

- *stat’ing the multi line extra file*No such file or directory*
- *Socket Read Error*
- *Errors reported by ITA Manager on production?Failure*
- *Remote client has disconnected*

To configure ITA Error criteria, add the desired text in the Intruder Alert Errors to Monitor box, as illustrated below.

Figure 6-5 ITA Error criteria



Select to specify case sensitive text matching.

Type error message text.

Click to add the entry to the selection criteria.

SELECT: Intruder Alert Error(s)
☑ Case Sensitive
New Entry
Add to List ->
Intruder Alert Errors to Monitor:
Edit List
Remove
Clear List

ITA Command criteria

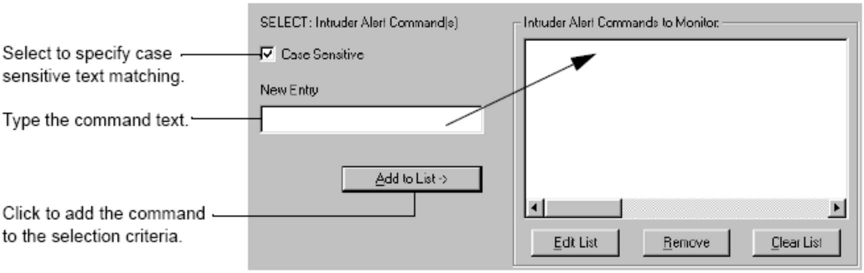
ITA!

The ITA Command criteria uses commands sent from Intruder Alert Event Viewer, using the Send Intruder Alert Command function. An Intruder Alert command is a user-defined word or phrase.

This criteria is used to test and debug policies. However, it may be used to perform a certain action, such as lower a raised flag or cancel a timer.

To configure the ITA Command criteria, add the desired text in the Intruder Alert Commands to Monitor box, as illustrated below.

Figure 6-6 Select Intruder Alert command criteria



SELECT: Intruder Alert Command(s)
☑ Case Sensitive
New Entry
Add to List ->
Intruder Alert Commands to Monitor
Edit List
Remove
Clear List

Select to specify case sensitive text matching.

Type the command text.

Click to add the command to the selection criteria.

Enter one or more code words or phrases to be selected or ignored. The following are example commands:

- cancel timer
- test
- page admin

Flag criteria

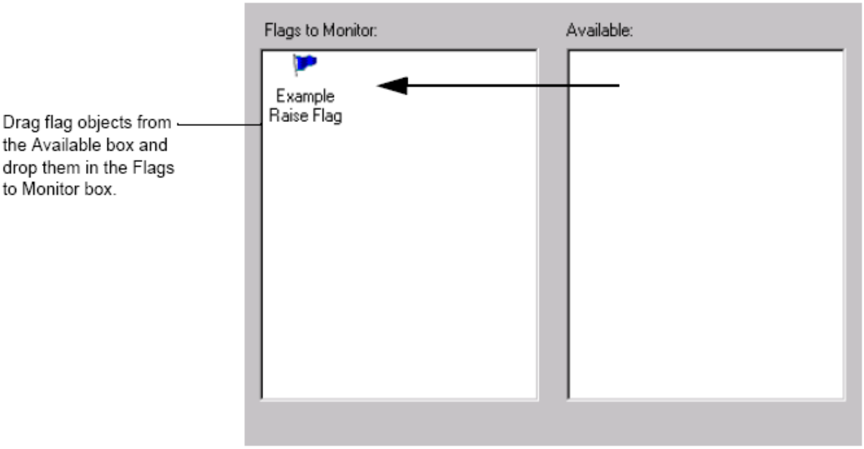
The Flag criteria selects or ignores flags raised by another rule. Intruder Alert lists the available flags in the Available box.

Flags can be used at two levels of selection. The first level is the flag itself. If the flag is raised, the selection criterion is met and, barring any ignore clauses, the rule's actions will be executed. The second level uses a feature called Event Context Capturing. This feature works with a raised flag to trigger only when certain conditions on the raised flag exist.

For event context capturing to work, the Raise Flag action must be configured to capture events. Then, you must configure the Select/Ignore flag with the desired selection criteria. The Raise Flag action and the Select/Ignore Flag criteria must reside in two separate rules.

To configure the Flag criteria at the basic level (event context capturing is not used), drag the desired flag from the Available box to the Flags to Monitor box as illustrated below.

Figure 6-7 Flag criteria

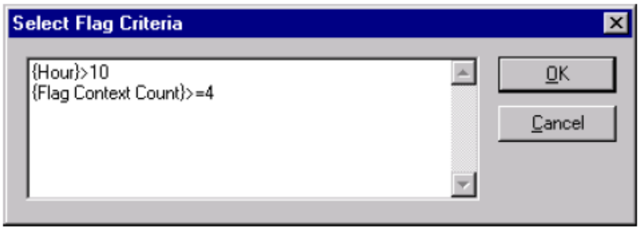


Drag flag objects from the Available box and drop them in the Flags to Monitor box.

If more than one flag is being monitored, use the And and Or radio buttons (located near the flag's Label field) to define the relationship between each of the selected flags. Choose the And radio button when all the selected flags must be raised to satisfy the requirements. Choose the Or radio button when any one of the selected flags alone is sufficient.

To configure the Flag criteria for event context capturing, drag the desired flag from the Available box and drop it in the Flags to Monitor box. Then, double-click on the flag's icon. When you double-click on the icon, the Select Flag Criteria dialog box appears.

Figure 6-8 Select Flag criteria dialog box



```
{Hour}>10
{Flag Context Count}>=4
```

The Select Flag criteria dialog box is used to define the flag's selection criteria. In the above example, the selection criteria for that flag will be met when four or more events occur after 10:00 am. When the hour is stored from a Select Flag criteria, it displays in GMT time. Defining the flag criteria allows event context capturing to work.

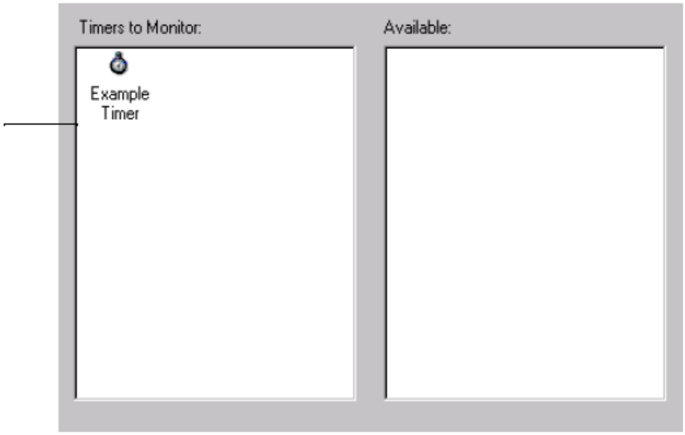
See "Event context configuration" on page 155.

Timer criteria

The Timer criteria selects one or more active timers. When the selected timer expires, the actions defined in the rule will execute. Timer criteria applies only to Select criteria.

To configure the timer, drag the timer object from the Available box and drop it in the Timers to Monitor box.

Figure 6-9 Select Timer criteria



Drag the timer objects from the Available box and drop them in the Timers to Monitor box.

If more than one timer is being monitored, use the And and Or radio buttons to define the relationship between each of the selected timers. Choose the And radio button when all the selected timers must expire to satisfy the requirements of this clause. Choose the Or radio button when one of the selected timers alone is sufficient to satisfy this criteria.

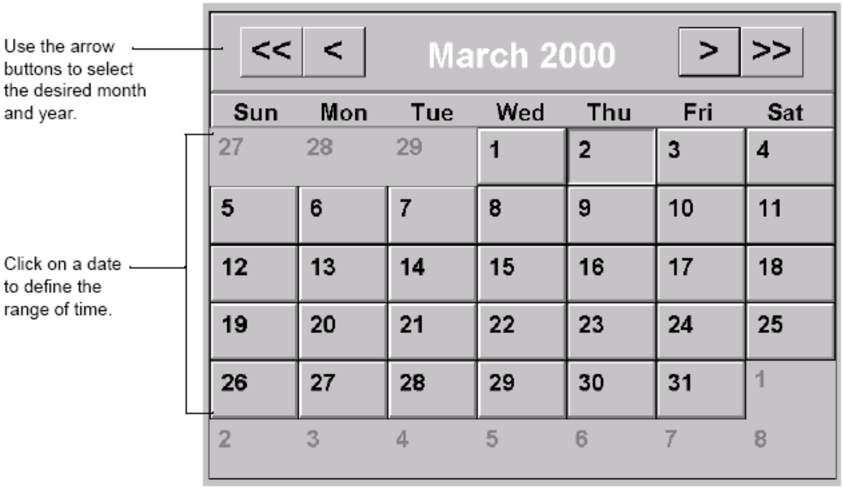
Date criteria

The Date criteria selects or ignores events occurring within a range of time, and must be used in conjunction with other selection criteria. It cannot be the sole selection criteria. The range of time may span seconds, minutes, hours, days, months, and even years.

The Date criteria is often used to build “working-hours,” “weekend-only,” and “after-hours” policies. For example, using the Date criteria with login policy rules, you can monitor all remote logins that occur from 6:00 pm on Friday to 8:00 am on Monday morning. Any remote logins that occur within that time would be detected. Remote logins during the work week would be ignored by that same policy.

To configure the date, select the desired years, months, and days; then select the desired hours, minutes, and seconds. When you select date, the date calendar appears.

Figure 6-10 Select Date criteria



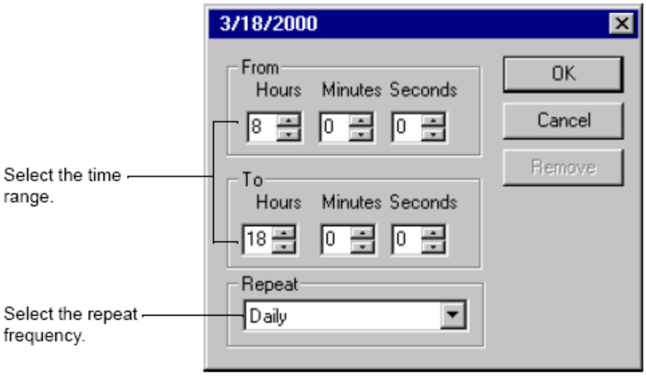
Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

Use the arrow buttons to select the desired month and year.

Click on a date to define the range of time.

When you click on a date in the calendar, the following time definition dialog box appears.

Figure 6-11 Time Definition dialog box



From: Hours 8, Minutes 0, Seconds 0

To: Hours 18, Minutes 0, Seconds 0

Repeat: Daily

Event date and time stamps

The Agent reports events using its own local time. The events display in the Event Viewer with the Agent's local time converted to the time zone of the Event Viewer. This allows the Event Viewer to report all events simultaneously as they happen, regardless of the time zone of the individual Agent.

This feature is rendered useless if the Agent is not set to its local time zone. The event report results become confusing when an Agent, or multiple Agents, with incorrect time zone settings report to the Event Viewer.

The Windows system default calendar for the United States is the Gregorian calendar.

To select a range or time and frequency

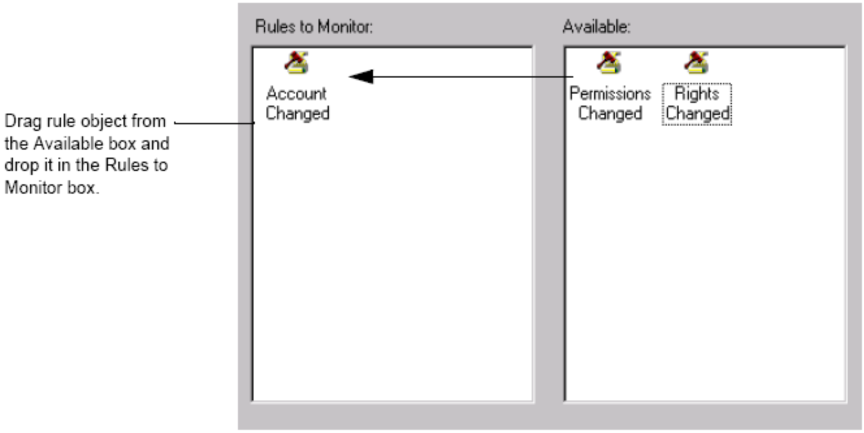
1. In the Date criteria configuration calendar, select the starting year and month and then click the desired day. Use the double arrows [<< or >>] to change the year and the single arrows [< or >] to change the month.
2. In the Time Definition dialog box, in the From boxes, select the starting time.
   Specify the time based on a 24-hour clock (military time).
3. In the To boxes, select the ending time.
   You cannot specify a range that overlaps another day. The range must be within 0 to 23 hours, 59 min, and 59 sec, on a specified day.
4. In the Repeat drop-down list, select the range of time.
5. Click **OK**.
   A red box appears on the calendar for the selected day. The red box indicates the selection for that day.

ITA Rule criteria

The Rule criteria selects or ignores another rule. In other words, the Select and Ignore criteria for another rule are referenced.

To configure, drag the desired rule from the Available box and drop it in the Rules to Monitor box, as illustrated below.

Figure 6-12 ITA Rule criteria



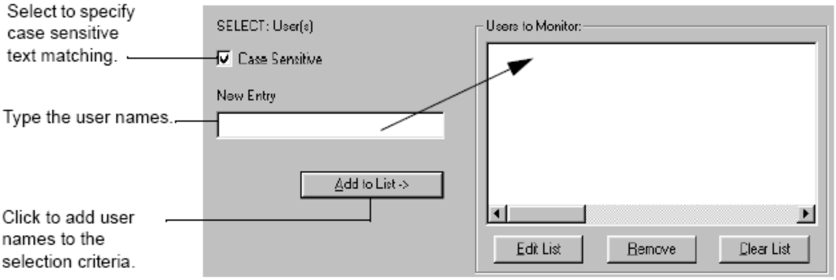
Drag rule object from the Available box and drop it in the Rules to Monitor box.

You can add more than one rule in the Rules to Monitor box. The And and Or radio buttons, located near the rule's Label field, define the functional relationship between multiple selected rules. Choose the And radio button when all the selected rules must be triggered to satisfy the requirements of this clause. Choose the Or radio button when one of the selected rules alone is sufficient to satisfy this criteria.

User criteria

The User criteria selects or ignores events generated by specified users, and must be used in conjunction with other selection criteria. To configure the User criteria, add the desired user names to the Users to Monitor box, as illustrated below.

Figure 6-13 Select User criteria



The User criteria supports case sensitive text matching and wildcard operators. Select the check box if you want the event text search to be case sensitive. Use (*) in place of multiple characters or names, and (?) in place of single characters.

Note: The availability of the username depends on the event. If the event contains the username, you can select and ignore based on username. If the event does not contain the username, this criteria should not be used. Windows does not always provide username information.

Be aware that parsing information with the audit log will not produce user names, even if it is parsed with that field.

System criteria

The System criteria selects or ignores specific Agent systems. System uses the Agent's name as the selection criterion. The Agent's name is determined internally by the Agent; it does not search event messages to determine the Agent's name.

Note: Because the Agent's name is determined internally, the System criteria may be the only Ignore criteria, but it should not be the rule's only Select criteria. Another type of Select criteria must be used in conjunction with a System criteria.

When configuring this criteria, the available systems include only those registered to a Manager. Thus, the list of available systems will vary from Manager to Manager.

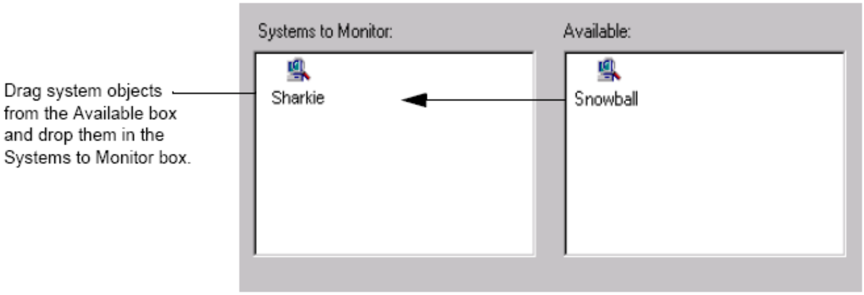
When adding the System criteria to a policy, you should configure it when the policy resides on the Manager, not when it resides in the Policy Library. The policy is located in the Manager's Policies branch and the available Agent systems are displayed in the Available box.

If you are creating your policy in the Policy Library, no systems will be displayed and you will need to finish the configuration of any System clauses when the policy has been copied to a Manager's Policies branch.

If the criteria exists with no Agent systems selected, it will be inactive and unable to detect anything.

To configure the System criteria, drag the desired system icons from the Available box and drop them in the Systems to Monitor box, as illustrated below.

Figure 6-14 System criteria



Drag system objects from the Available box and drop them in the Systems to Monitor box.

If more than one Agent system is being monitored, the And/Or radio buttons define the relationship between the selected systems. Choose the And radio button when all selected systems must be present to satisfy the requirements of this selection criteria. Choose the Or radio button when one of the selected systems alone is sufficient.

Windows Registry Key criteria

R

The Windows Registry Key criteria selects or ignores events generated in the registry by key. With these criteria, the system can act on signatures that indicate unauthorized access to the system. The Windows Registry Key criteria can apply any action and report to the Intruder Alert Event Viewer.

Actions

Actions execute when the Select criteria are true and the Ignore criteria are false. Intruder Alert offers 14 different actions. This section describes the purpose of each action and how to configure it.

The actions are:

- Record to Event Viewer
- Raise Flag
- Lower Flag
- Send Email
- Send Page
- Append to File
- Notify
- Start Timer
- Execute Command
- Run Shared Action action
- Cancel Timer
- Kill Process
- Disconnect Session
- Disable User

Note: The ITA Shared Actions policy allows you to administer actions from a central location.

See "Modify the ITA Shared Actions policy" on page 141.

Record to Event Viewer

The Record to Event Viewer action records events in an event database located on the Manager's system. Intruder Alert's Event Viewer queries the event database to generate online and printed reports.

When adding the Record to Event Viewer action to a rule, no configuration is required. The action need only be present to log events in the Manager's event database. However, you can tag additional data to the event by specifying a label-data pair in the Enter Record Information box. The added text only appears in the Event Viewer's text view.

Use the following format for label-data pairs:

<Desired Label Name>=<Desired Data/Text>

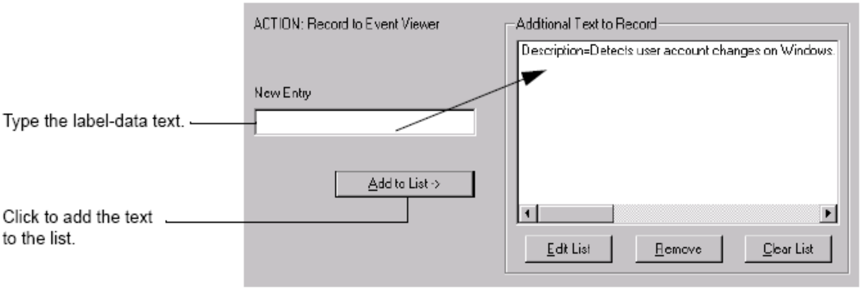
See the following examples:

- Computer_Name=adminbox
- threat_type=network
- Description=Agent detected 3 failed administrator logins

Note: For multiple-word labels, use an underscore character (_) between words. Spaces between words are not allowed. The data portion allows up to 256 characters.

To append additional text to an event message, add the desired data-label statement to the Additional Text to Record box, as illustrated below.

Figure 6-15 Record to Event Viewer action fields



ACTION: Record to Event Viewer

Addtional Text to Record

Description=Detects user account changes on Windows.

Type the label-data text.

Click to add the text to the list.

See “Understand and manage the event database” on page 261.

Raise Flag

The Raise Flag action can be used to:

- Create an electronic marker indicating that an event occurred
  Rules located within the same policy can select the raised flag to trigger other actions.
- Notify other Agents reporting to the same Manager that an event occurred
  Flags can be raised globally on all Agents reporting to the same Manager. Global flags allow Agents to work together to detect complex, multiple-system events. Global flags are useful for detecting events occurring on different systems throughout the enterprise. Events occurring on a single system may not be indicative of a larger attack; however, when combined together, each piece completes the profile of the attack, such as an attacker attempting by brute force to gain access to various systems on the network (detected through multiple failed logins).
- Perform event context capturing
  The Raise Flag action has the ability to capture and store events. This feature is called event context capturing. With event context capturing, you can configure a Select criteria or Ignore criteria flag to trigger when certain conditions on a raised flag exist.
  See "Configuring the Raise Flag action to use event context capturing" on page 165.

Note: Use global flags judiciously. Raising flags globally increases network traffic. With global flags it is possible to flood the network (and all the Agents that report to the configured Manager) with large numbers of TCP/IP packets.

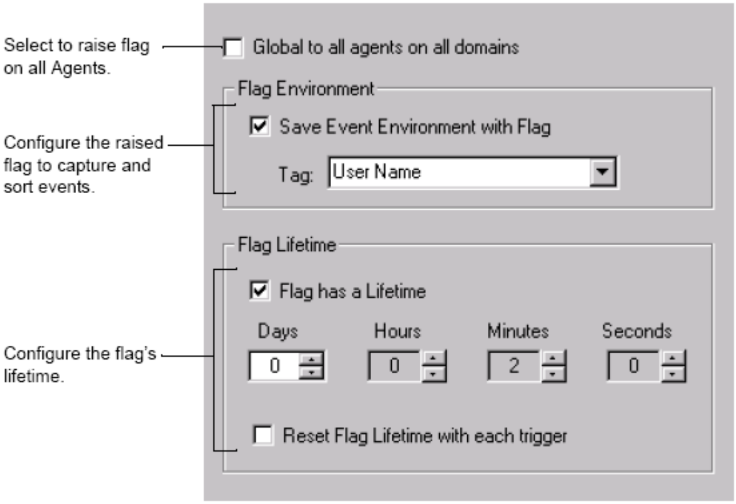
Flags can be raised for finite or infinite periods of time. If the flag is raised indefinitely, the only thing that can lower the flag is a Lower Flag action.

See "Lower Flag" on page 110.

If the raised flag is given a lifetime, then the flag will remain raised until the lifetime expires. Flags configured with lifetimes can also be canceled by a Lower Flag action.

The following graphic illustrates the raise flag configuration fields.

Figure 6-16 Raise Flag action



Select to raise flag on all Agents.

Configure the raised flag to capture and sort events.

Configure the flag's lifetime.

□ Global to all agents on all domains

Flag Environment

☑ Save Event Environment with Flag

Tag: User Name

Flag Lifetime

☑ Flag has a Lifetime

Days	Hours	Minutes	Seconds
0	0	2	0

□ Reset Flag Lifetime with each trigger

The following table describes each field.

Table 6-3 Raise Flag configuration options

Option	Description
Global to all Agents on all domains	This setting directs the Agent to raise the same flag globally on all Agents registered to the same Manager. **Note:** Global flags and event context capturing (enabled via the Save Event Environment with Flag check box) cannot be enabled at the same time.
Save Event Environment with Flag	This check box directs the Agent to save event contexts with the raised flag. It is used to enable the event context capturing feature. See "Configuring the Raise Flag action to use event context capturing" on page 165.
Tag	This box allows you to select the criteria by which events will be sorted on the raised flag. For example, if you select User Name, events captured during the flag's lifetime will be sorted by user name.
Flag has a Lifetime	This check box enables/disables the flag's lifetime. Check this option to configure the flag with a lifetime. After checking this box, specify the flag's lifetime in the Days, Hours, Minutes, and Seconds fields.

Table 6-3 Raise Flag configuration options

Option	Description
Days, Hours, Minutes, Seconds	These fields define the flag's lifetime.
Reset Flag Lifetime with Each Trigger	This option directs the flag to reset its lifetime with each new trigger that occurs while the flag is raised. For example, if the flag has a lifetime of two minutes and two events occur, one minute apart, that trigger the flag, the first event raises the flag and the second resets the flag's timer back to two minutes. Thus, the flag's total lifetime is three minutes. Use this option when you want the flag's lifetime to reset with each new trigger that occurs during its lifetime.

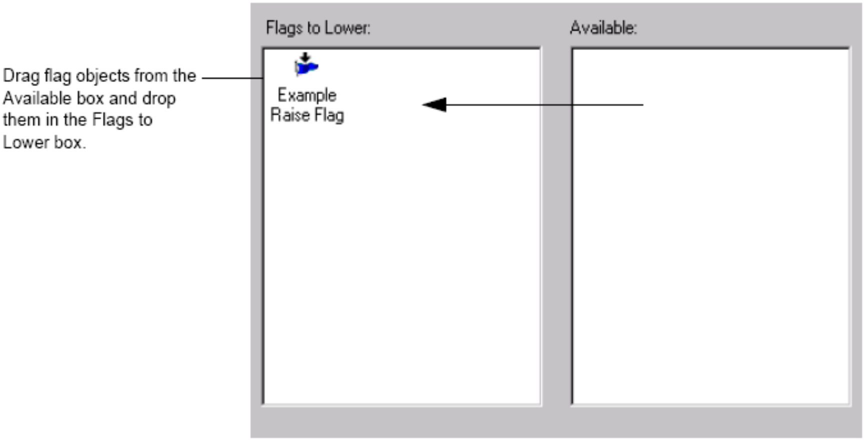
Lower Flag

The Lower Flag action lowers or cancels a raised flag.

Note: If the raised flag has any events or contexts saved, all contexts will be deleted when the flag is lowered.

To configure the Lower Flag action, drag the desired flags from the Available box and drop them in the Flags to Lower box, as illustrated below.

Figure 6-17 Lower flag action


Drag flag objects from the Available box and drop them in the Flags to Lower box.
Flags to Lower:
Available:
Example Raise Flag

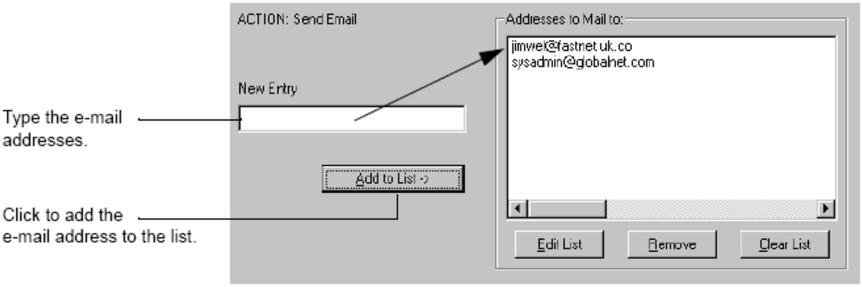
Send Email

The Send Email action emails the event message to a specified user or group of users. Emails can only be sent by Agents configured with the ability to send email. Each Agent that has a policy containing a Send Email action should be configured with email capabilities.

See “Configuring the Agent for email notification” on page 83.

To configure the email action, list the email recipient’s email address or addresses in the Addresses To Mail To box, as illustrated below.

Figure 6-18 Send Email action



jimwel@fastnet.uk.co
sysadmin@globalnet.com

Use the standard email address syntax:

(<name>@<domain name>)

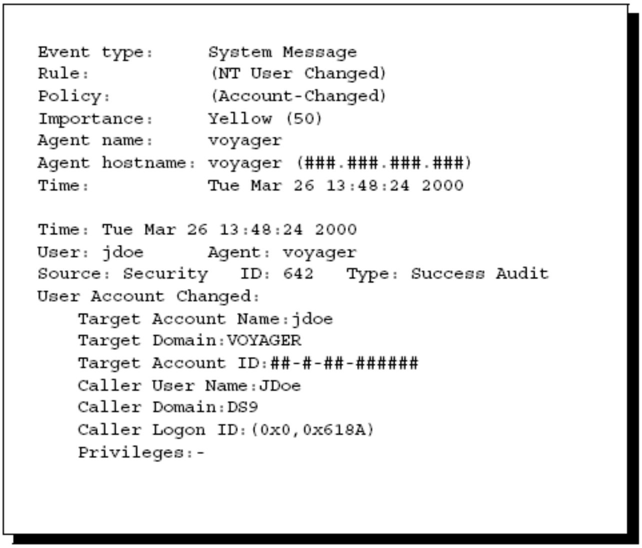
when configuring the action criteria. For example:

johndoe@symantec.com

Note: The Send Email action can also be used to send email to alphanumeric paging devices in lieu of a modem for paging, provided the email server supports this feature, and is properly configured to do so.

The following graphic depicts an example email message sent by Intruder Alert.

Figure 6-19 Example email message



```
Event type:      System Message
Rule:            (NT User Changed)
Policy:          (Account-Changed)
Importance:      Yellow (50)
Agent name:      voyager
Agent hostname:  voyager (###.###.###.###)
Time:            Tue Mar 26 13:48:24 2000

Time: Tue Mar 26 13:48:24 2000
User: jdoe       Agent: voyager
Source: Security   ID: 642   Type: Success Audit
User Account Changed:
    Target Account Name:jdoe
    Target Domain:VOYAGER
    Target Account ID:##-#-##-######
    Caller User Name:JDoe
    Caller Domain:DS9
    Caller Logon ID:(0x0,0x618A)
    Privileges:-
```

Note: Use this action sparingly. If a rule's selection criteria is too broad— meaning that a large number of events trigger the rule— then large numbers of email messages will be sent. A prolonged implementation (which may be seconds, or days depending on the selection criteria) may yield undesired results, including slowed performance by the Agent; diminishing performance by the email server; and diminished network performance due to a large volume of email messages. Limit your use of this action to prevent system problems.

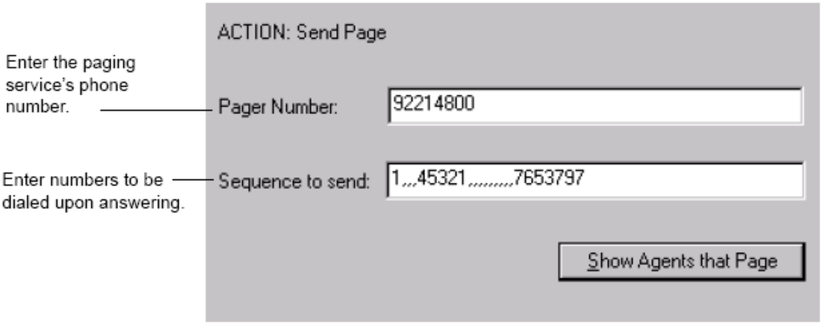
Send Page

The Send Page action calls a pager via a modem set up on an Agent system. For the pager action to function, one or more Agents connected to a Manager must to be configured with a modem capable of paging, plus, the Agent must to be configured to interface with the modem device.

See "Configuring the Agent for pager notification" on page 84.

To configure the Send Page action, type the numbers required to reach your paging service in the Pager Number field. Be sure to include any prefacing numbers required for dialing outside the organization. (The number nine [9] is often used in many organizations to get an outside line.) Then, in the Sequence To Send field, type the dialing sequence required for sending the page to the desired administrator.

Figure 6-20 Send page action



ACTION: Send Page

Pager Number: 92214800

Sequence to send: 1,,,45321,,,,,,,,,,7653797

Enter the paging service's phone number.
Enter numbers to be dialed upon answering.
Show Agents that Page

Configuration Guidelines

Paging action configuration guidelines are as follows:

- In the Pager Number field, add any prefacing numbers necessary to obtain an outside phone line.
- In the Sequence to Send field, enter the numbers necessary, separated by commas, to select options and send messages through the paging service. Commas act as one second delays.
  Most paging services have options that must be entered after the call has been answered (for example, press "1" to page, press "2" to speak with an attendant, etc.). In addition, some paging services accept numbers

immediately following each other without having to wait for options to be presented; however, many do not.

Some services do not require that you wait for an option to be presented before being able to choose it. In these circumstances, you must configure pauses in the sequence. Pauses are configured using commas. The length of the pause depends on the modem; however, as a rule of thumb, use one comma for every second.

- Always test the policy to verify that the Send Page action is configured properly.

Append to File

The Append to File action writes events in a user-specified text file. The location of the file may be on a local or remote host configured with an Intruder Alert Agent.

Note: For security reasons, the directory or folder where the file will reside must already exist. Intruder Alert will create the file, but it will not create the directory.

To append events in a file located on the local system, specify the desired path and file name, for example:

- On UNIX:
  /axent/ita/system/<hostname>/collect.log
- On Windows:
  <system disk>:\Program Files\Symantec\ITA\system\<hostname>\collect.log

To append events to a file on a remote Agent system, use the following format:

<path and file name>@<Agent label>

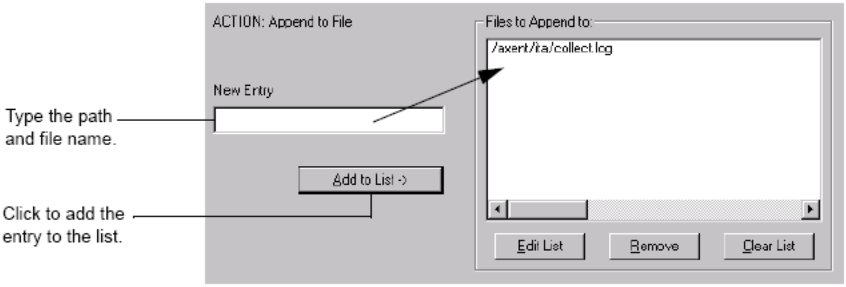
For example:

- On UNIX:
  /axent/ita/system/<hostname>/collect.log@sharkie
- On Windows:
  c:\logs\logname.log@minnow

Note: Each record in the log file represents a single message. Records are separated by a line of equal signs (=). Use the Append to File action sparingly. If a rule's selection criteria is too general, meaning a large number of events trigger the rule, the log file will fill up. A prolonged implementation (which may be seconds or days depending on the selection criteria) may yield undesired results, including slowed performance by the Agent, diminishing disk space (i.e., the log file grows consuming valuable disk space), and diminished network performance if the log file is on a remote system.

To configure the Append to File action, add the desired path and file name to the Files To Append To box, as illustrated below.

Figure 6-21 Append to File action



/axent/ita/collect.log

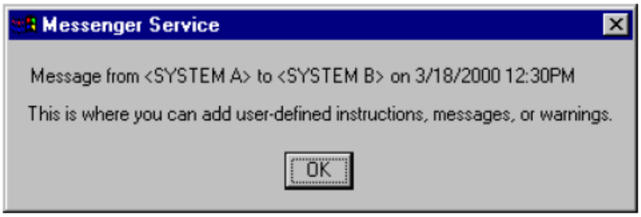
Type the path and file name.

Click to add the entry to the list.

Notify

The Notify action sends an on-screen message to a specified user or system. It can include user-defined instructions, messages, event descriptions, or warnings. The following graphic illustrates an on-screen message generated on Windows.

Figure 6-22 Example notification message on Windows



Message from <SYSTEM A> to <SYSTEM B> on 3/18/2000 12:30PM

This is where you can add user-defined instructions, messages, or warnings.

Note: If the user is not logged on or the system is not turned on, the notification will be lost. Therefore, a Notify action should not be the only action taken.

Supported formats for notifying a user include:

- <User Name>
  Specifying a user name instructs Intruder Alert to notify a specific user. The user must be logged in to receive the notification.
  Examples include:
  - johnd
  - alincoln
- {user}
  The variable “{user}” instructs Intruder Alert to send the notification message to the user who generated the system message. For example, you can send a message to a user who attempts to change a user account. However, note that in some situations the user name may not be known. If the user name can be determined via the operating system collector, this variable will notify the user. If it cannot, no message will be sent.
  Remember to use braces ({}), not brackets ([]).

  Note: In UNIX environments, where syslog has been centralized on a single UNIX system, the notification message may be lost.
  If the user is logged on to multiple Window systems residing on the same Domain Controller, the notification message may appear on any one of those systems, but it will not display on all the systems the user is logged into.

- <User Name>@<Agent Label>
  The <User Name>@<Agent Label> command instructs Intruder Alert to notify a specific logged-on user on a remote system on which an Agent is running. If the user is not logged on, the message will be lost. Do not make this the only source of notification for important messages.

The Agent label must be the actual name of the Agent as it appears in Intruder Alert. The IP address or email domain name will not work.

Examples include:

- jdoe@musicbox (Generic Use)
- jondoe.rcbl.accntg.novell@enterprise (NDS Format)
- alincoln@accounts.utah.globalco (Long Agent Name)

- <User Name>@{Agent Label}

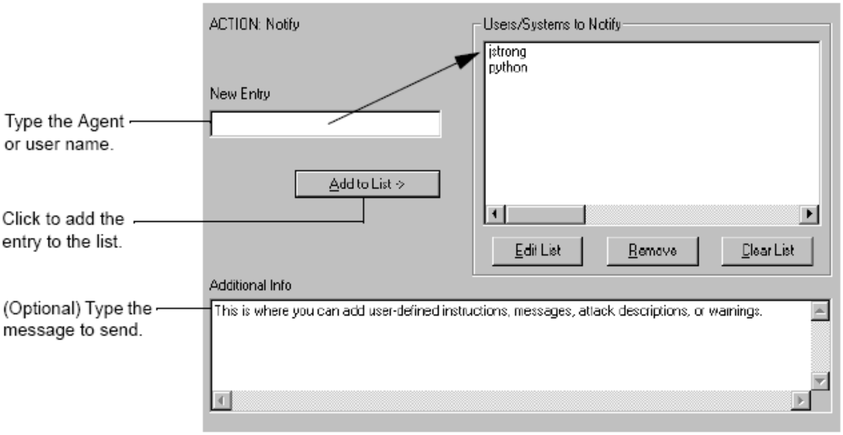
  This option directs Intruder Alert to send notification to a specific user logged on to the system where the event was read by an Agent. If the user is not logged in, the notification message will be lost.

  Examples include:

  - johnd@{Agent Label} (Generic Use)
  - davber.rcvbl.accntg.novell@{agent label} (NDS format)

To configure a Notify action, add the user and system names to the Users/ Systems to Notify box and then type additional text in the Additional Info box, as illustrated below.

Figure 6-23 Notify action



jstrong
python

This is where you can add user-defined instructions, messages, attack descriptions, or warnings.

Type the Agent or user name.

Click to add the entry to the list.

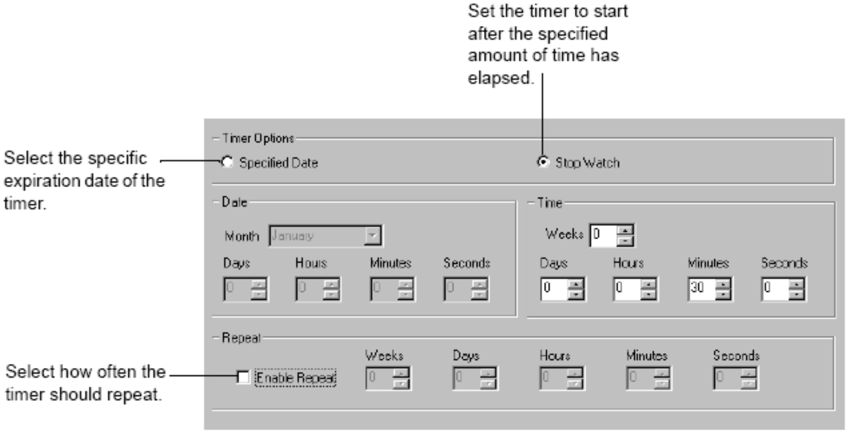
(Optional) Type the message to send.

Start Timer

The Start Timer action starts a timer that counts down to either a specified date or for a specified amount of time. The Start Timer action works with a Select Timer criterion located in a separate rule; the Select Timer criterion detects when the timer expires.

Like flags, timers are used internally by the Agent. There is no graphical representation indicating they have started, or how much time is remaining on them. Timers can be set to repeat on a specified frequency once they have expired. Timers expire, or are cancelled by the Cancel Timer action.

Figure 6-24 Start Timer action



Set the timer to start after the specified amount of time has elapsed.

Select the specific expiration date of the timer.

Select how often the timer should repeat.

Timer Options: ○ Specified Date ● Stop Watch

Date: Month January; Days 0; Hours 0; Minutes 0; Seconds 0

Time: Weeks 0; Days 0; Hours 0; Minutes 30; Seconds 0

Repeat: □ Enable Repeat; Weeks 0; Days 0; Hours 0; Minutes 0; Seconds 0

With the Specified Date radio button selected, the timer will expire on a specific month, day, and time. With the Stop Watch radio button selected, the timer will count down the specified amount of time.

Execute Command

The Execute Command action executes an operating system command, script file, or executable file.

On UNIX systems, the Execute Command action can execute any command, program, or shell script. Scripts must not require user interaction. Specify the full path name to the command or script file, for example:

/usr/bin/myscript

On Windows, the Execute Command action can execute the following types of executable files:

- .cmd
- .bat
- .exe
- .com

They must not require user interaction. Use the file path name to the executable file, for example:

c:\scripts\ita\security.bat

The following table lists and defines available variables.

Table 6-4 Execute command variables

Variable	Definition
{user}	The user name from the triggering event. If the user name is included in the event, this information can be used.
{event file}	The name of a temporary file in the TEMP directory that contains the text of the triggering event. Using the {event file} variable, you can pass the entire event message into another process. In that process, the data can be parsed and used in a wide-range of applications. The temp file itself must be manually deleted.
{process ID}	The process identification number (PID). The process that generated the event.
{session ID}	The session identification number (SID). The session that generated the event.
{agent label}	The name of the Agent as it is known by Intruder Alert. This may or may not be the system name.
{host name}	The name of the system or host on which the event occurred.
{system softid}	The IP address.
{time}	The time the event occurred.

Using these variables, event information can be passed from Intruder Alert to another process. This could be an application such as HP OpenView or MS Access, or an operating system command. Data is written to a temp file, parsed by an external program, then passed on command.

For example, you could write a command that copies the user names associated with a particular event to a text file. HP OpenView or some other program would then read the file and use that information.

The following examples show ways in which these variables may be used:

- kill {process ID}
- echo {host name} >>/tmp/myfile
- load {event file}

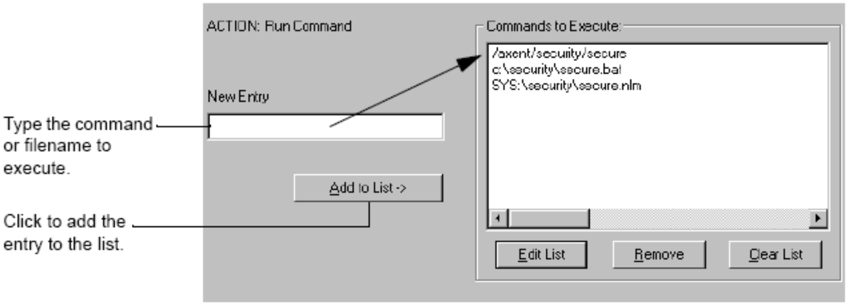
Note: On Windows, for Intruder Alert Agents to execute the commands in the Execute Command action, these commands must also be listed in the commands.txt file located in the directory:

<system disk>:\Program Files\Symantec\ITA\system\<System Name>

See “Securing the Execute Command action” on page 131.

To configure an Execute Command action, add the desired commands or the path and file name of the executable files you want Intruder Alert to execute.

Figure 6-25 Execute Command action



```
/axent/security/secure
c:\security\secure.bat
SYS:\security\secure.nlm
```

Type the command or filename to execute.

Click to add the entry to the list.

Note: The configured commands may not execute in the desired order. Therefore, when the order of execution is important, you should consider placing the commands in multiple rules that use flags and timers to execute the commands in the desired sequence.

Also, make sure the policy is activated on the operating system that supports the specified commands. For example, it will do no good to activate an Execute Command action containing UNIX commands on a Windows system.

Temporary event file cleanup

In an Execute Command action, if the user has the event file variable in the command to execute, a temporary file in the OS specific temp directory is created to hold the event information. A new temporary file is created for each event.

The event file contains a copy of the event text. The file name is then passed to the script to be used by the executable program. The Agent has no way of knowing when the script of the executable starts, so the Agent does not own the task of cleaning up. Intruder Alert was designed so that the script or executable becomes responsible for post process cleanup once it has finished with the file.

Securing the Execute Command action

The Execute Command action has an enhanced security feature. It allows you to control which commands may be executed by Intruder Alert Agents.

The Execute Command action is secured by listing the allowed commands in the commands.txt file, then securing that file's access from anyone other than Intruder Alert Agents and a highly trusted security administrator. The commands.txt file is installed with each Intruder Alert Agent and, on Windows, appears in the directory:

<system disk>:\Program Files\Symantec\ITA\system\<System Name>

See "Securing the Execute Command action" on page 131.

Run Shared Action action

The Run Shared Action action executes an action contained in another rule or policy residing on the Agent system. Having a shared action makes a group of policies' actions easier to maintain, because content is changed in only one location.

Configuration guidelines

When creating shared actions, the following criteria must be met:

- The rule with the shared action must begin with the word "Shared:" The colon must be included. For example:
  Shared: Priority One Alert

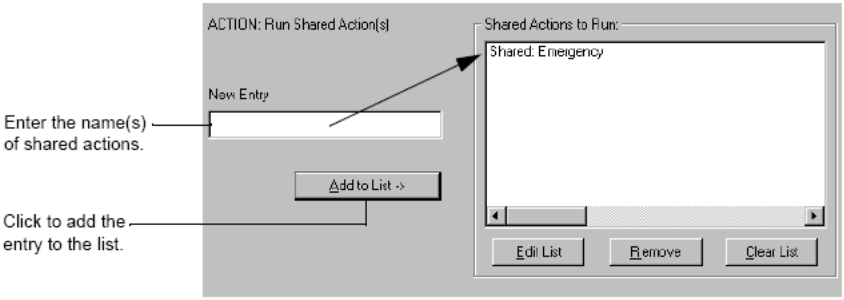
- The Run Shared action must reference the shared rule. Specifically, the Run Shared action must list the shared rule's name exactly as it appears in the tree view).
- The policy containing the shared action must reside on the Agent system.

Note: The ITA Shared Actions policy contains ten rules. Each rule is designed for different types of notification. Rather than creating your own shared rules, you can modify and use these rules according to your needs. In addition, if you need more shared action rules, you can add them to the ITA Shared Actions policy. This way all shared rules will be located in the same policy. To ensure the ITA Shared Actions policy is active on all Agents, activate it on the All Agents domain.

See "Modify the ITA Shared Actions policy" on page 141.

To configure this action, type the name of the rule containing the desired action in the Shared Actions to Run box, as illustrated below.

Figure 6-26 Run Shared actions


ACTION: Run Shared Action(s)
New Entry
Add to List ->
Shared Actions to Run:
Shared: Emergency
Edit List
Remove
Clear List
Enter the name(s) of shared actions.
Click to add the entry to the list.

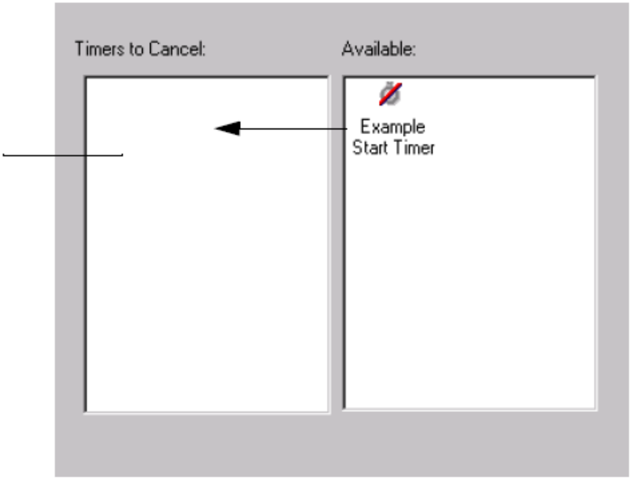
Cancel Timer

The Cancel Timer action cancels or deletes an active timer.

Note: Canceling timers and flags after the event allows Intruder Alert to start with a clean slate. If you do not cancel active timers after an attack, subsequent events may yield false-positive results.

To configure the Cancel Timer action, drag the desired timer objects from the Available box and drop them in the Timers to Cancel box.

Figure 6-27 Cancel Timer action



Drag timer objects from the Available box and drop them in the Timers to Cancel box.

Kill Process

The Kill Process action stops the process that triggered the event. However, the Kill Process action cannot stop all processes.

On UNIX systems, this action kills a specific process when the event contains a process identification (PID) number, “PID: #####.” If a PID does not exist in the event, the process cannot be killed. Not all variants of UNIX use the PID.

Windows does not provide the specific process that generated the event. As a result, Intruder Alert cannot kill a Windows-specific process. Rather, Intruder Alert has been designed to terminate all processes belonging to the user associated with the event. Therefore, the selection criteria must contain the user name. If the user name is not available processes will not be stopped. However, under no circumstances can this action kill a process associated with an administrator account.

Because NetWare does not allow one process to kill another, this action cannot operate on NetWare systems, but there is an alternative solution.

See “Disconnect Session” on page 124.

Disconnect Session

The Disconnect Session action stops all processes that have the same user name or session ID as the process that generated the event.

On UNIX systems, this action can terminate a specific session if the event contains a session identification (SID) number, “Session ID: XXXXX.” If the event does not contain a session ID, sessions cannot be disconnected.

On Windows systems, the Disconnect Session action kills all processes associated with the user name contained in the event; therefore, the selection criteria must contain the user name. If the user name is not available, no processes will be stopped. On Windows systems, the disconnect session cannot kill a process associated with an administrator account.

Note: On Windows systems, the user will be able to log in again. If you want to prevent the user from logging in, combine a disable user account action with a Disconnect Session action.

See “Disable User” on page 124.

On NetWare, this action disconnects the session if the event contains the connection number. Therefore, the selection criteria must be triggered by events containing a connection number.

Disable User

The Disable User action disables a user’s account—other than an account having root (UNIX) or administrator (Windows) privileges.

On Windows systems, this action disables the account of the user associated with the account—so the user will not be able to log in again until the account is reactivated by a system administrator.

Note: This action does not immediately log the attacker off the system. If you want to log them off the system, add a Disconnect Session action clause with the disable user account action.

See “Disconnect Session” on page 124.

Administering policies

This chapter includes the following topics:

Applying policies to a domain

Policies are applied to all Agents in a domain. Once a policy is applied to an Agent, the Agent begins monitoring for the defined Select and Ignore criteria.

Note: A policy is not enforced until it is applied.

The following instructions describe the process for applying a policy from the Policy Library. However, if the policy already exists on the Manager, it can be applied from the Policies branch.

To apply a policy that already exists on the Manager from the Policies branch, begin at Step 4 in the procedure below.

To apply a policy to one or more domains

1 Connect to a Manager.
See "Connecting to a Manager" on page 64.

2. In the Intruder Alert tree, in the Policy Library branch, click the desired policy.
3. Do one of the following:
   - Drag the policy from the Policy Library and drop it on the Policies branch under the desired Manager.
   - Copy and paste the policy from the Policy Library to the Policies branch of the desired Manager.

   The policy now resides on the Manager, but it has not yet been applied.
4. In the Policies branch, right-click the desired policy and then click **Apply to Domain** in the drop-down list.
5. In the Apply Policy to Domain dialog box, do one of the following:
   - Click the desired domain and then click **OK**.
   - Press **Ctrl** and select multiple domains and then click **OK**.

   You can apply the policy to one or more domains on the connected Manager.

To simultaneously apply multiple policies

1. If you have not already connected to a Manager, complete the steps shown in the section:

   See “Connecting to a Manager” on page 64.
2. In the Intruder Alert tree, in the Policy Library branch, do one of the following:
   - Press **Shift** and select the first and last of a group of desired policies.
   - Press **Ctrl** and select multiple policies.
3. Do one of the following:
   - Drag the policies from the Policy Library and drop them on the Policies branch under the desired Manager.
   - Copy and paste the policies from the Policy Library to the Policies branch of the desired Manager.

   The policies now reside on the Manager, but have not yet been applied.
4. In the Intruder Alert tree, right-click the desired domain and then click **Apply Policies** in the drop-down list.
5. Do one of the following:
   - Press **Shift** and select the first and last of a group of policies to apply.
   - Press **Ctrl** and select multiple policies to apply.
6. Click **OK**.

Removing policies from a domain

Removing a policy removes it from all Agents in the selected domain. Once removed, the Agent no longer monitors for the conditions specified in the policy.

To remove a policy

1. Connect to a Manager.
   See "Connecting to a Manager" on page 64.
2. In the Intruder Alert tree, in the Domains branch of the connected Manager, expand the domain.
3. In the domain branch, expand **Policies in Domain** to view policies applied to that domain.
4. Right-click the policy and then click **Remove from Domain** in the drop-down list.
   The policy is removed from the domain, but it still resides on the Manager in the Policies branch. You can also delete the policy from the Manager.
   See "Deleting policies from a Manager" on page 130.

To simultaneously remove multiple policies from a domain

1. In the Intruder Alert tree, in the desired domain under the Domains branch of the connected Manager, click **Policies in Domain**.
   The configuration frame in the right pane displays all of the policies applied to the domain.
2. In the right pane, do one of the following:
   - Press **Shift** and select the first and last of a group of policies to remove.
   - Press **Ctrl** and select multiple policies to remove.
3. On the keyboard, press **Delete**.
4. In the confirmation dialog box, click **OK**.
   Although you are asked to confirm the deletion of the policies, the policies themselves are not deleted from the Policies branch under the Manager. They are removed only from the domain.

Moving policies to the Policy Library

When a policy is no longer used, you can store it in the Policy Library if it does not already reside there, export it, or delete it from the Manager.

To keep the policy, store it in a folder in the Policy Library or export it to an archive before deleting it from the Manager. If you delete it without storing it in a folder in the Policy Library, or exporting it to an archive, the policy will be permanently deleted.

To move a policy to the Policy Library

1. In the tree, in the Policies branch, click the policy.
2. On the menu bar, do one of the following:
   - Click **Edit > Cut**
   - Click **Edit > Copy**
3. In the Policy Library branch, click the folder where you want to store the policy.
4. On the menu bar, click **Edit > Paste**.

Deleting policies from a Manager

To delete a policy from a Manager

1. In the Policies branch under the Manager, click the policy.
2. On the toolbar, click **Delete**.
3. In the confirmation dialog box, click **Yes**.

Exporting policies

You should export your customized policies before upgrading to a new release or before transferring them to another installation of Intruder Alert Administrator. Intruder Alert policy files can be exported from the Manager or Policy Library and saved.

Note: Before uninstalling Intruder Alert, export any policies you wish to keep, including user-defined, modified, or otherwise valuable policies to a storage location outside of the Symantec\ITA directory. Otherwise, during the uninstallation process, these files will be deleted.

To export a policy

1. In the Policy Library branch or a Manager’s Policies branch, click the policy.
2. On the menu bar, click **File > Export Policy**.

3 In the Exporting Policies dialog box, browse to the folder in which to save the policy.

4 In the File Name text box, type the policy name.

5 In the Save as Type text box, type or select **.pol**.

6 Click **Save**.

Importing a policy

You may upgrade or expand the monitoring capability of Intruder Alert by importing new or custom policies. Policies can be imported into a folder in the Policy Library branch or a Manager's Policies branch. Policies must have a .pol file extension to import successfully.

To import a policy

1 In the Intruder Alert tree, do one of the following:

   - In the Policy Library branch, click one of the folders.
   - In the Managers branch, under the desired Manager, click **Policies**.

2 On the menu bar, click **File > Import Policy**.

3 In the Importing Policies dialog box, browse to the location of the policy to import, and click the policy.

4 Click **Open**.
The policy is imported and stored in the selected branch.

Securing the Execute Command action

The Execute Command action has an enhanced security feature to prevent Intruder Alert from being used incorrectly. This feature allows you to control which commands may be executed by Intruder Alert Agents.

The Execute Command action is disabled by default, and is enabled only through a list of allowed commands in the commands.txt file. That file is secured from access by anyone other than Intruder Alert Agents and a highly trusted security administrator.

The commands.txt file is installed with each Intruder Alert Agent and appears in the following directory for each operating system:

■ UNIX:	/axent/ita/system/<hostname>
■ Windows:	<system disk>:\Program Files\Symantec\ITA\system\<hostname>

Each line in the file lists a separate command. For each command, you must use the full path and file name, including file extensions such as .exe, .bat, and .nlm. Do not include comments (#) in front of the path name. Type only the absolute path name.

On UNIX, if you create a script file to be executed by Intruder Alert, begin the file with #!/bin/sh on the first line of the script so that Intruder Alert will be able to execute the command. You may need to change the file permissions to make the script executable.

To add entries to the commands.txt file

1. On each Agent host where the commands will be executed, open the commands.txt file in a text editor capable of standard ASCII output.
   The commands.txt file is located in the following directories:
   - On Windows:
     <system disk>:\Program Files\Symantec\ITA\system\<hostname>\
   - On UNIX:
     /axent/ita/system/<hostname>/
2. Add a line to the end of the file, and type the fully qualified path and filename of the command, batch file, or script on that line. Command line parameters or switches are not required. Include file extensions, such as .exe, .bat, and .nlm.
   For example:
   ```
   /opt/security/disable
   c:\winnt\security.bat
   SYS:\setpass [event file]
   ```
3. Repeat step 2 for each command.
4. Save the commands.txt file.
5. Do one of the following to restart the Intruder Alert Agent:
   - On Unix, type the commands:
     ```
     /axent/ita/bin/itarc stop
     /axent/ita/bin/itarc start
     ```
   - On Windows, use Windows Services to restart the Agent.
     See "Configuring Agent service properties" on page 61.

Creating and modifying policies

This chapter includes the following topics:

The policy development process

Policies should be created by individuals who have a technical background and a thorough understanding of how Intruder Alert works.

Note: Before creating a new policy, make sure that Intruder Alert does not already have a solution for the security problem you are trying to detect. Visit the Symantec Web site for the latest policy developments. Access the web site at:

http://securityresponse.symantec.com

Under Updates, click Symantec Intruder Alert.

Before creating policies, you should:

- Be familiar with how Intruder Alert collects events on each supported operating system.
- Have a good understanding of rule functionality.
- Be familiar with Intruder Alert's Select, Ignore, and Action criteria.

Suggestions for policy development

Keep in mind the following tips when developing policies:

- Keep the size of your policy files below 64K.

  The maximum size of a policy file is 64K. If you have multiple rules within the policy, group related rules together into multiple, smaller policy files.

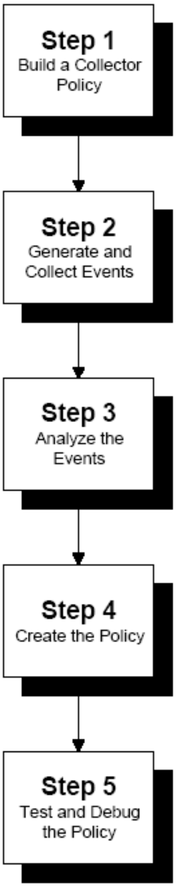
- Avoid circular policies.

  A circular policy runs many times consecutively. This policy configuration error can create unnecessary peaks in CPU utilization and consumes unwarranted disk space. If you experience either of these problems, examine your customized policies for circular logic.

  See "Circular policies" on page 136.

The following graphic illustrates the main steps for creating a new policy.

Figure 8-1 Steps for creating a policy



Building a collector policy

A collector policy gathers all system messages and appends them to a user-defined log file. Security administrators analyze the events captured by the collector and identify events that make up an event signature. These selected events become the building blocks for rules and policies.

See “Creating and configuring a collector policy” on page 144.

Generating and collecting events

Collect events by activating the policy on a domain and performing the actions that generate the events. Try to isolate the events by minimizing the number of Agents in the domain, and minimizing the time that the collector policy is activated. Otherwise, the Event Viewer or Append-to-File log will be flooded with events.

Analyzing the events

You can use the following questions to help analyze events:

- What events were generated by your actions?
- When did the events occur in relation to each other?
  If more than one event was captured, did those events occur in a specific sequence? If so, how far apart?
- Where and on what systems did they occur?
  During the analysis phase you should identify all the relevant information needed to create the policy.

Creating the policy

After analyzing the events and learning what events identify the performed action, the next step is to create the policy in Intruder Alert. However, before creating a policy, you must know the logic behind Intruder Alert rules and the various building blocks for creating rules.

See "Policies, rules, and criteria" on page 91.

Testing and debugging the policy

After the policy has been created, activate it on a domain, perform the same actions as before, and verify that it captures the desired events. Resolve any problems that might arise.

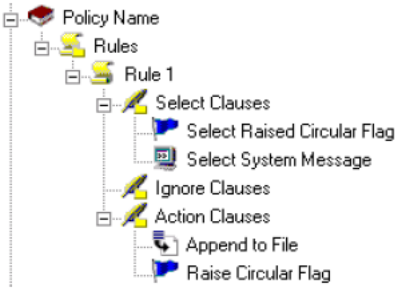
Circular policies

A circular policy runs many times consecutively, which can cause peak CPU utilization and consume excessive disk space. If you experience either of these problems, examine your customized policies for circular logic. The following is an example of a circular policy.

Select criteria:	Select system message for event A; Select raised flag 1
Action:	Append event to file and raise flag 1

The following diagram illustrates what this policy looks like in the Intruder Alert tree.

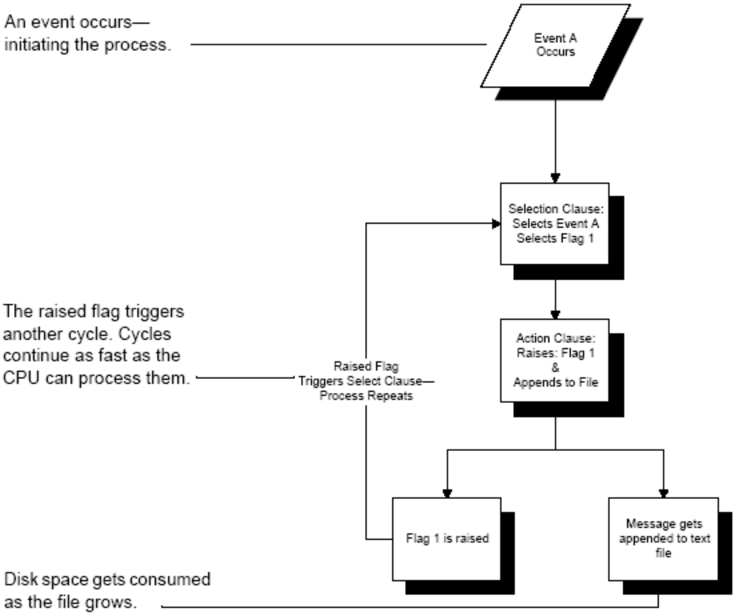
Figure 8-2 Intruder Alert Tree / Circular Policy



- Policy Name
  - Rules
    - Rule 1
      - Select Clauses
        - Select Raised Circular Flag
        - Select System Message
      - Ignore Clauses
      - Action Clauses
        - Append to File
        - Raise Circular Flag

The following diagram illustrates how this policy operates.

Figure 8-3 Circular policy diagram


An event occurs—
initiating the process.
Event A Occurs
Selection Clause: Selects Event A Selects Flag 1
The raised flag triggers another cycle. Cycles continue as fast as the CPU can process them.
Raised Flag Triggers Select Clause— Process Repeats
Action Clause: Raises: Flag 1 & Appends to File
Flag 1 is raised
Message gets appended to text file
Disk space gets consumed as the file grows.

In this example, the policy selects an event. The actions append the event to a log file and raise a flag, completing the first cycle. The second cycle begins when the system detects the raised flag and appends another event to the log file and raises the flag again. Additional cycles continue as fast as the system can process the events. These cycles cause peak CPU utilization, while the Append to File action keeps writing events to the text file, consuming disk space.

Suggestions for managing policies

The following suggestions may help you to manage your policies:

- Upgrade Intruder Alert from earlier versions to version 3.6.1.
- Apply tune-up packs as they become available.
- To customize a policy, copy it and modify the copied version.
- When applying a policy, verify that you are not applying both an original and a modified version of the same policy.

Policy development tasks

To develop policies, there are a number of tasks you need to perform. This section describes the following tasks:

- Creating a policy
- Adding and deleting a rule
- Adding and deleting rule criteria
- Saving policy changes
- Modify the ITA Shared Actions policy
- Creating and configuring a collector policy
- Creating a new folder in the Policy Library

Creating a policy

The following instructions describe the process of creating a new policy.

To create a policy in Intruder Alert

1. If you have not already done so, connect to the Manager.
   See "Connecting to a Manager" on page 64.
2. In the Intruder Alert tree, expand the Manager's branch to display the Policies branch.
3. Right-click **Policies** and then click **New** in the drop-down list.
   Intruder Alert adds a new policy to the tree as New Policy1.
4. In the right pane, in the Label text box, type a name for the new policy.
5. In the Description text box, type a description of the new policy.
6. In the Intruder Alert tree, click **New Policy1** to update the name.
   The new name replaces New Policy1 in the Policies branch.

7 To save the policy, right-click the policy in the Intruder Alert tree and then click **Save** in the drop-down list.
Intruder Alert adds a pencil to the policy icon in the tree when the policy needs to be saved.
The next step is to add one or more rules to the new policy.
See "Adding and deleting a rule" on page 139.

Adding and deleting a rule

The following procedures describe the processes of adding a rule to, and deleting a rule from, a policy.

To add a rule

1 In the Intruder Alert tree, expand the Manager's branch to display the Policies branch.

2 Expand **Policies** and then expand the desired policy's branch.
The Rules branch should be visible.

3 Right-click **Rules** and then click **New** in the drop-down list.
Intruder Alert adds a new rule added to the Intruder Alert tree as New Rule.

4 In the right pane, in the Label text box, type a name for the new rule.

5 In the Description text box, type a description for the new rule.

6 Optionally, in the Rule Value boxes, set the rule values.
Possible values range between 0 and 100.
For more information about rule values and how to use them, see the section:
See "Rule value" on page 93.

7 Optionally, to set the rule type, check **Indirect**, **Filter**, or **Disable Rule Usage**.
For more information about these Rule Usage check boxes, see the section:
See "Rule type" on page 94.

8 To save changes to the policy, right-click the policy and then click **Save** in the drop-down list.
Intruder Alert adds the new rule to the policy.
The next step is to add criteria to the rule.
See "Adding and deleting rule criteria" on page 140.

To delete a rule

1 Expand the tree to view the rule.

2 Right-click the rule and then click **Delete** in the drop-down list.

3 In the dialog box, click **Yes** to confirm the deletion.

Adding and deleting rule criteria

Each rule must contain one or more Select criteria and one or more actions. A rule can optionally contain Ignore criteria. This section describes how to add criteria or actions to, and delete criteria or actions from, a rule.

Intruder Alert's out-of-box policies can be configured with additional actions, such as email capabilities and paging.

See "Policies, rules, and criteria" on page 91.

To add criteria or actions to a rule

1 In the Intruder Alert tree, in the Policies branch, expand the policy and then expand **Rules**.

2 Expand the desired rule to display the Select, Ignore, and Actions branches.

3 Do one of the following:

- Right-click **Select** and then click **New** and the desired Select criteria in the drop-down list.
- Right-click **Ignore** and then click **New** and the desired Ignore criteria in the drop-down list.
- Right-click **Actions** and then click **New** and the desired Action in the drop-down list.

4 In the right pane, configure the criteria or action as needed.

5 Repeat the above steps until all desired criteria and actions are added.

6 To save changes to the policy, right-click the specific policy and then click **Save** in the drop-down list.

To delete criteria or actions from a rule

1 Expand the tree to view the specific criteria or action.

2 Right-click the criteria or action and then click **Delete** in the drop-down list.

3 In the dialog box, click **Yes** to confirm the deletion.

Saving policy changes

After creating or modifying a policy from the Policies branch on the Manager you must save the changes, otherwise the changes will be lost. If the policy is already activated on a domain, saving the changes activates those changes on the policies that reside on the Agent. You know that changes need to be saved when a pencil appears on the policy's icon.

If the policy has not been saved before you exit Intruder Alert Administrator, you will be prompted to save. You may save all, or discard all changes to the policies.

To save changes to a policy

1. Expand the tree to view the policy.
   If a pencil appears on the policy icon, then there are changes that need to be saved.
2. Do one of the following:
   - Right-click the policy and then click **Save** in the drop-down list.
   - On the toolbar, click **Save**.

Modify the ITA Shared Actions policy

The ITA Shared Actions policy administers actions from a central location. You can modify one rule in the ITA Shared Actions policy and have it affect every policy configured to use it.

The ITA Shared Actions policy resides in the Configure to Detect> Generic branch in the Policy Library branch. This section describes its purpose and how to modify it for your organization's needs.

Note: All out-of-box policies in versions 3.0 and 3.01 were configured to use the ITA Shared Action policy. However, if that policy was mistakenly removed, or is not configured to detect, then all policies configured to use it would be rendered ineffective. Therefore, to avoid this type of mistake, all out-of-box policies in version 3.6.1 are configured with their own actions. However, the ITA Shared Action policy is still included and activated automatically so all version 3.0 policies will function in version 3.6.1

The ITA Shared Actions policy includes rules defining a different type of response. For example, you could configure the Shared: Emergency rule to send email to an administrator.

The following table describes the intended use for each rule.

Table 8-1 ITA Shared Actions policy

Rule	Description
Shared:Append to Agt	This rule appends captured events to a file located on the Agent's system. You can specify any directory and file name you wish. Be sure to modify the path and file name according to the Agent's operating system.
Shared:Append to Mgr	This rule appends captured events to a file located on the Manager's system. Use the format: <path and file name>@<Manager's Name> For example on Windows: c:\Program Files\Symantec\ITA\bin\logfile@Mars
Shared:Email	This rule sends an email to one or more people. Configure the Send Email action with the desired email addresses. Note: The Agent must be configured with email capabilities. See "Configuring the Agent for email notification" on page 83.
Shared:Exec Command	This rule executes a command. For instructions on how to configure the Execute Command action, see the section: See "Execute Command" on page 118.
Shared:Notify System	This rule notifies a system. For help on how to configure the Notify action, see the section: See "Notify" on page 115.
Shared:Record Alert	This policy records events having a moderate security threat in the Manager's event database by using the Record to Event Viewer action. The rule value is set at 50.
Shared:Record Emergency	This policy records events posing a high security threat in the Manager's event database by using the Record to Event Viewer action. The rule value is set at 90.
Shared:Record FYI	This policy records events posing a low security threat in the Manager's event database by using the Record to Event Viewer action. The rule value is set at 20.

Instead of creating your own shared rules, you should modify and use existing rules according to your needs. You can modify shared rules within the Policy Library, and then copy them to the desired Managers.

Note: Intruder Alert Administrator automatically saves all changes that you make within the Policy Library. However, once you copy a policy to a Manager's branch, you must explicitly save it and any changes to it. Administrator sends policy updates to the Manager only after you save.

To ensure that the ITA Shared Actions policy is available to all Agents, apply it in the All Agents domain.

To configure a shared rule

1. In the Intruder Alert tree, expand **Policy Library** and then expand **Configure to Detect**.
2. In the Configure to Detect branch, expand **Generic** and then expand **ITA Shared Actions**.
3. In the ITA Shared Actions branch, expand **Rules**.
   The shared rules should be visible.
4. Expand the desired rule to display the Select, Ignore, and Actions branches.
5. Expand **Actions**.
   The configured actions are displayed.
6. Do one of the following:
   - To reconfigure an existing action, click the action to view the configuration fields in the right pane of Intruder Alert Administrator, and configure as necessary.
     For more information about a particular action, see the desired heading in the section:
     See "Actions" on page 106.
   - To add a new action, right-click **Actions** and then click **New** and the desired action in the drop-down list. Configure the action as necessary.
   - To delete an action, right-click the particular action and then click **Delete** in the drop-down list. In the Delete dialog box, click **Yes**.

   The changes are automatically saved.
7. Copy the policy to the desired Manager's branch and then apply it to the All Agents domain.
   See "Applying policies to a domain" on page 127.

To add a new shared rule

1. In the Intruder Alert tree, expand **Policy Library** and then expand **Configure to Detect**.

2 In the Configure to Detect branch, expand **Generic** and then expand **ITA Shared Actions**.

3 In the ITA Shared Actions branch, right-click **Rules** and then click **New** in the drop-down list.
The new rule is added to the Rules branch as New Rule.

4 In the right pane, in the Label text box, type "Shared:" (be sure to add the colon) and then whatever name you desire.
For example:

- Shared: Priority 1 Alert
- Shared: Email Admin
- Shared: Page Admin

5 In the tree, click **New Rule**.
This updates the rule name and expands the branch.

6 Add and configure the desired actions to the new rule.
Rules with shared actions do not require Select and Ignore criteria.
The rule is automatically saved.

7 Copy the policy on the desired Manager's branch and then apply it to the All Agents domain.
See "Applying policies to a domain" on page 127.

Creating and configuring a collector policy

The following instructions describe how to create and configure a collector policy. A collector policy captures all event messages. There are three different types of collector policies you can create. The following table describes each collector.

Table 8-2 Collector types

Collector type	Description
System Message	The System Message collector uses operating system log files to capture all system events.
Status Message	The Status Message collector uses Intruder Alert status messages from Manager and Agent log files to capture all Intruder Alert status events.
ITA Error Message	The ITA Error Message collector uses Intruder Alert error messages from Manager and Agent log files to capture all Intruder Alert error events.

Note: Because collectors gather all events, carefully select where the policy is activated and for how long. If activated on a busy domain, the collector will gather large amounts of data, making analysis difficult.

To create a collector policy

1. In Intruder Alert Administrator, in the tree, do one of the following:
   - In the Policy Library branch, right-click an existing folder and then click **New Policy** in the drop-down list.
   - In a connected Manager branch, right-click **Policies** and then click **New** in the drop-down list.
2. In the right pane, in the Label text box, name the policy.

   Symantec suggests naming the System Message Collector “Collector,” the Status Collector “Status Collector,” and the ITA Error Collector “ITA Errors Collector.”
3. Optionally, in the Description text box, type a description of the policy.

   Adding a description causes the policy name to be updated in the tree.
4. In the tree, if necessary, click **New Policy** to update it with the new name, and then expand the branch.
5. Under the new policy, right-click **Rules** and then click **New** in the drop-down list.
6. In the right pane, in the Label text box, for the rule name, type:

   `Collector`
7. In the tree, click **New Rule** to update it with the name “Collector”.
8. Under the Collector rule, do one of the following:
   - To create a System Message collector, right-click **Select** and then click **New > System Message** in the drop-down list.
   - To create a Status Message collector, right-click **Select** and then click **New > ITA Status Message** in the drop-down list.
   - To create an ITA Error Message collector, right-click **Select** and then click **New > ITA Error** in the drop-down list.
9. In the collector configuration fields in the right pane, click in the New Entry box, type an asterisk (*) and then click **Add to List**.

   An asterisk is an Intruder Alert wildcard operator. By itself it tells the Agent to select or capture all messages.
10. In the tree, in the Collector rule branch, click **Actions**.
11. In the Action toolbar above the right pane, click **Record to Event Viewer**.

The changes are automatically saved.
When activated, the policy records events to the Event Viewer.

Creating a new folder in the Policy Library

Create new folders in the Policy Library branch to organize user-defined policies or reorganize Intruder Alert's out-of-box policies.

To create a new folder in the Policy Library

1. In the Policy Library branch, do one of the following:
   - Right-click Policy Library and then click New Folder in the drop-down list.
   - Right-click an existing folder under Policy Library and then click **New Folder** in the drop-down list.
2. In the right pane, in the Label text box, name the new folder.
3. In the tree, right-click **New Folder** to update the name and save the change.
   Policies can be created in or pasted to this folder.

File and directory security

This chapter includes the following topics:

Intruder Alert file monitoring

Intruders often attempt to replace critical system files with Trojan horse versions or alter system files in an effort to create a back door for future intrusions. They may also try to replace Web files with slanderous versions to defame or sabotage an organization's credibility.

Intruder Alert is preconfigured to detect changes to mission-critical files on UNIX, and Windows systems. Additional configuration steps are usually not necessary. Symantec security experts have defined a set of mission-critical files that are automatically monitored via the UNIX File Tampering and Windows File Tampering policies. These policies are automatically activated during Agent Installation.

If you have other important files that you want Intruder Alert to monitor, you can create additional "file watch" lists and configure Intruder Alert to monitor those lists. Intruder Alert supports multiple file watch lists.

Intruder Alert can determine if a file (text file, program, configuration file, etc.) or directory has disappeared, reappeared, or changed (been accessed or modified).

This security process works by comparing the attributes of files and directories with the file attribute database. If an actual file or directory structure differs from the database, the process sends a message to the Agent to indicate the file has changed.

Intruder Alert uses Coordinated Universal Time (UTC) (also known as Greenwich Mean Time (GMT)) when storing and comparing file attributes such as the creation, access, or modification times of monitored files. Filewatch events shown in the text view portion of the Event Viewer are displayed in local time. File modification and creation times are shown in GMT in the message text portion of the Event Viewer.

The monitoring feature can be configured to monitor a number of individual file attributes. The following table lists the file attributes that the process can monitor.

Table 9-1 File monitoring capabilities

Available on both platforms	Available on UNIX only
Checksum (WROT, BROT, MD5)	Group (gid)
Deletion	Owner (uid)
File size	Permissions (rwx)
Modified time	Driver description
Read-only	
Access time	
Creation time	
Permissions (r)	
File location	
Links (hard and symbolic)	
File type	

The UNIX File Tampering and Windows File Tampering policies detect and respond to changes in the monitored attributes of the default file watch lists.

If you create additional file watch lists, you must also create and activate a new policy to detect and respond to changes in those lists.

The following sections describe how to create a file watch list. You can also modify an existing file watch list.

See “Modifying a file watch list” on page 154.

Configuring Intruder Alert file monitoring

Configuring Intruder Alert to monitor a list of files consists of the four steps that are outlined below:

- Creating a file watch list
- Adding the filewatch command to ita.ini
  Examples include:
  - filewatch=c:\security\ita\filewatch\chk1hr.lst,chk1hr
  - filewatch=/security/ita/filewatch/filechk.fil,filechk
  - filewatch = c:\security\ita\filewatch\test.lst,test
- Restarting the Manager and Agent to activate the new command added to the ita.ini.
  See "Starting and stopping Managers/Agents" on page 66.
- Creating and activating a policy to detect the new event messages, and to perform desired actions.
  See "Creating a policy" on page 138.

Creating a file watch list

The file watch list defines:

- The files to check
- The types of checks to perform
- The frequency with which to check the files

Text messages sent to the Agent "Byte" Rotary (BROT), Word Rotary (WROT), MD5 checksums, and file access time are configurable. Do not use checksums and access times together, because checksums regularly access the file. The check time and the number of files to check will impact CPU usage. Shorter times and longer file lists will have the greatest impact.

The following table describes the commands and options used in the file watch list.

Table 9-2 File watch list commands and options

Command format	Description
%<text>	This command adds a text comment to the list. Text comments can be added anywhere in the list. They must be preceded by a percent symbol (%).

Table 9-2 File watch list commands and options

Command format	Description
$TIME = <integer>	The $TIME command defines the number of seconds between scans. Use the $TIME command only once in a list.
$RESCAN	The $RESCAN command directs Intruder Alert to re-scan directories and files that contain wildcards. An asterisk (*) directs the process to list all files and subdirectories. A question mark (?) can replace single variable characters.
$MESSAGE <text>	The $MESSAGE command defines a character string that will be appended to the event message. The message will be used in the selection criteria of a policy rule.
$BROT	This command enables and disables Byte Rotary (BROT) checksums. The command functions like a toggle switch. Each time the monitoring process encounters the command in the list, the BROT checksum will be switched on or off. An additional toggle ";BROT" can be placed on individual files and directories. This parameter should be added to the end of the directory or file command, for example: c:\security\bin\syntech.exe;BROT
$WROT	This switch functions the same as $BROT to start, skip, or stop Word Rotary (WROT) checksums. Like BROT, WROT has an additional toggle that can be placed on individual files and directories. This switch is ";WROT." Use it in the same way as the BROT switch.
$MD5	This switch functions the same as $BROT to start, skip and stop MD5 checksums. Like BROT, MD5 has an additional toggle that can be placed on individual files and directories. This switch is ";MD5." Use it in the same way as the BROT switch.
$ACCESS	This command enables and disables the function that detects when files were last accessed. If enabled, access times on the files following the command are compared. Note: The monitoring process must access the file in order to calculate checksums. Therefore, do not enable both checksum and access functions at the same time.

Table 9-2 File watch list commands and options

Command format	Description
<path><filename>	Use the following guidelines: On UNIX, the root directory can be defined differently for each user. Use #rootdir as a variable location. On UNIX, you can use "/" to indicate the root directory. Use the variable "#windir" to identify the correct location and name of the main Windows directory. Use "#ita" to locate the ita directory dynamically. If the system name is part of the path, use the variable "#system" to represent the host name. If the platform is part of the path, use the variable "#platform" in place of the platform name. Wildcards (* and ?) are supported.

Two file watch lists are automatically installed with every UNIX and Windows Agent. On Windows, these lists reside in the folder:

<system disk>:\Program Files\Symantec\ITA\system\<hostname>

On UNIX, they reside in the directory:

axent/ita/system/<hostname>

You can use these files as a reference when creating your own file watch lists. The following table describes these files.

Table 9-3 Installed watch list files

Scan time	Files	Description
60 Seconds 30 Seconds	ntcrit_S.lst (Windows) uxcrit_S.lst (UNIX)	Contains mission-critical files.
8 Hours	ntcrit_L.lst (Windows) uxcrit_L.lst (UNIX)	Contains a list of important files to monitor.

Note: The ntcrit_S.lst and uxcrit_S.lst files have been optimized. Do not add files to these lists. You may add files to the ntcrit_L.list and uxcrit_L.lst files.

To create a file watch list

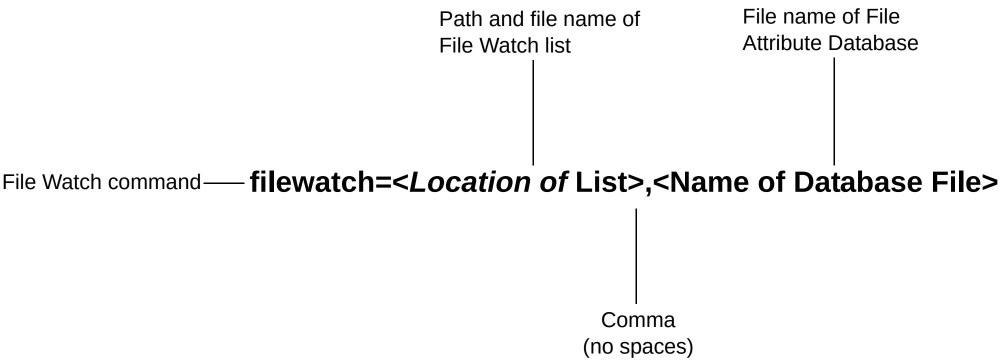
1. Create a new document in a UNIX or Windows text editor.
2. Enter any text comments. Precede text comments with a percent symbol (%).
3. Enter the **$TIME** = command and specify a value in seconds.
4. Optionally, if wildcards are going to be used when specifying the list of files, enter the **$RESCAN** command.
5. Specify the desired check summing or access function commands.
   The monitoring process must access the file in order to calculate checksums. Therefore, do not enable both checksum and access functions at the same time.
6. List the files to be checked.
   List one file or directory per line.
7. Optionally disable check summing.
8. Optionally enable access time monitoring.
9. Optionally list the files to be checked.
10. Optionally disable access time monitoring.
11. Save the file in standard ASCII file format with a .lst file extension.
    The file watch list may reside in any directory on the system. However, Symantec recommends storing it in the following locations:
    - On UNIX, in the directory:
      axent/ita/system/<hostname>
    - On Windows, in the folder:
      <system disk>:\Program Files\Symantec\ITA\system\<hostname>

    Once you have created the file watch list, you must direct the Agent to begin monitoring the selected files by adding a setting in the ita.ini file.
    See “Adding the filewatch command to ita.ini” on page 152.

Adding the filewatch command to ita.ini

The file watch list is enabled via a command located in the Agent’s ita.ini file. The following diagram illustrates the command’s syntax.

Figure 9-1 File watch command syntax


Path and file name of File Watch list
File name of File Attribute Database
File Watch command
filewatch=<Location of List>,<Name of Database File>
Comma (no spaces)

Examples include:

- filewatch=c:\security\ita\filewatch\chk1hr.lst,chk1hr
- filewatch=/security/ita/filewatch/filechk.fil,filechk
- filewatch = c:\security\ita\filewatch\test.lst,test

The process allows multiple file watch lists to be activated at the same time. Each file watch list should have its own line in the ita.ini file.

Note: When naming the File Attribute Database, do not specify a file extension. The process gives the File Attribute Database file a .fio file extension by default.

To add the filewatch command

1. Open the ita.ini file into a text editor.
2. Locate the "[Agent]" section and add the filewatch command.
3. Save changes to the ita.ini file.
   The filewatch command is now added to the ita.ini file. You must stop and restart the Manager and Agent to initiate the monitoring process for the selected files.
   See "Starting and stopping Managers/Agents" on page 66.
   In addition, you must create a policy that detects and responds to the file watch message.
   See "Creating a policy" on page 138.

Modifying a file watch list

You can modify an existing file watch list by adding or deleting files to check, changing the type of checks Intruder Alert performs, or changing the frequency with which Intruder Alert checks the files.

Note: Do not modify the ntcrit_S.1st or unxcrit_S.1st lists.

To modify a file watch list

1 Stop the Intruder Alert Manager and Agent.

2 Open the file watch list in a text editor.

3 Make the desired changes to the list.
See Table 9-2, "File watch list commands and options," on page 149.

4 Save the file.

5 Restart the Intruder Alert Manager and Agent.

Event context capturing

This chapter includes the following topics:

Understanding and using event contexts

Event context capturing enables Intruder Alert to remember certain events and distinguish between them for more refined selection and response. This feature is especially useful when a high volume of the same type of events occurs within a short period of time. For example, Intruder Alert can identify an attacker’s five failed logins from among 30 that occur within a three-minute period.

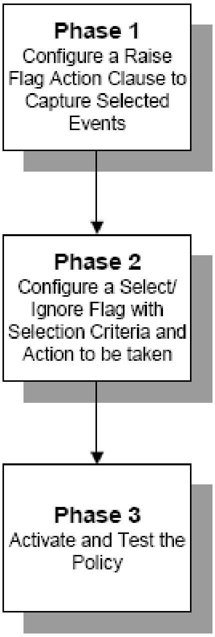
Before you begin creating or modifying policies to use event context capturing, you should thoroughly understand how it works. The next sections will teach you the principles of event context capturing:

- Event context configuration
- Event context capturing
- Event context selection criteria
- Notes and known issues

Event context configuration

Using event context capturing requires three configuration phases or steps, as illustrated in the following graphic.

Figure 10-1 Steps to configuring event context capturing


Phase 1
Configure a Raise Flag Action Clause to Capture Selected Events
Phase 2
Configure a Select/ Ignore Flag with Selection Criteria and Action to be taken
Phase 3
Activate and Test the Policy

The following list provides an overview to the process of configuring event context capturing:

- In a policy, create a rule with a Raise Flag action.
- Configure the rule to remember event contexts.
- Add Select criteria to the rule for an event that will trigger the Raise Flag action.
- In the same policy, create a second rule with a Select/Ignore Flag criteria.
- Configure it with the desired selection criteria and the action to be taken once the rule is triggered.
- Save, activate and test the policy to make sure it is detecting and responding to the event.

Event context capturing

It is important to understand that events occur within a context. Intruder Alert event messages describe much of the context in which they occur, such as:

- What type of event occurred

- When it happened
- The process that generated the event
- The user that generated the event
- The system on which the event occurred

Simply stated, an event context answers the who, what, when, where, why, and how of an event.

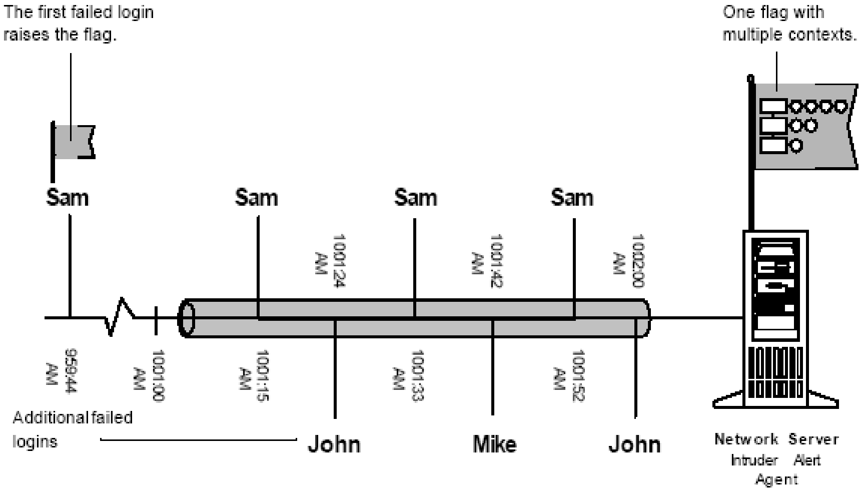
However, single events do not always comprise the event. More complex events generate multiple event messages, and only when analyzed together do they identify the event.

Intruder Alert has the ability to filter user-specified events by associating event contexts with a flag, as well as the ability to create multiple instances of a flag, save a flag count, and specify the lifetime of a flag.

Intruder Alert's Raise Flag action has the ability to capture events of interest and remember them to identify an event. When the events are saved with the Raise Flag action, the Select and Ignore Flag can be used to monitor the event and respond as soon as the event is identified.

To illustrate how event context capturing works, suppose you want to detect three failed logins by the same user within a two minute period. In the following illustration Sam, John, and Mike perform a total of seven failed logins within a four-minute period—between 9:59 am and 10:03 am.

Figure 10-2 Failed logins diagram

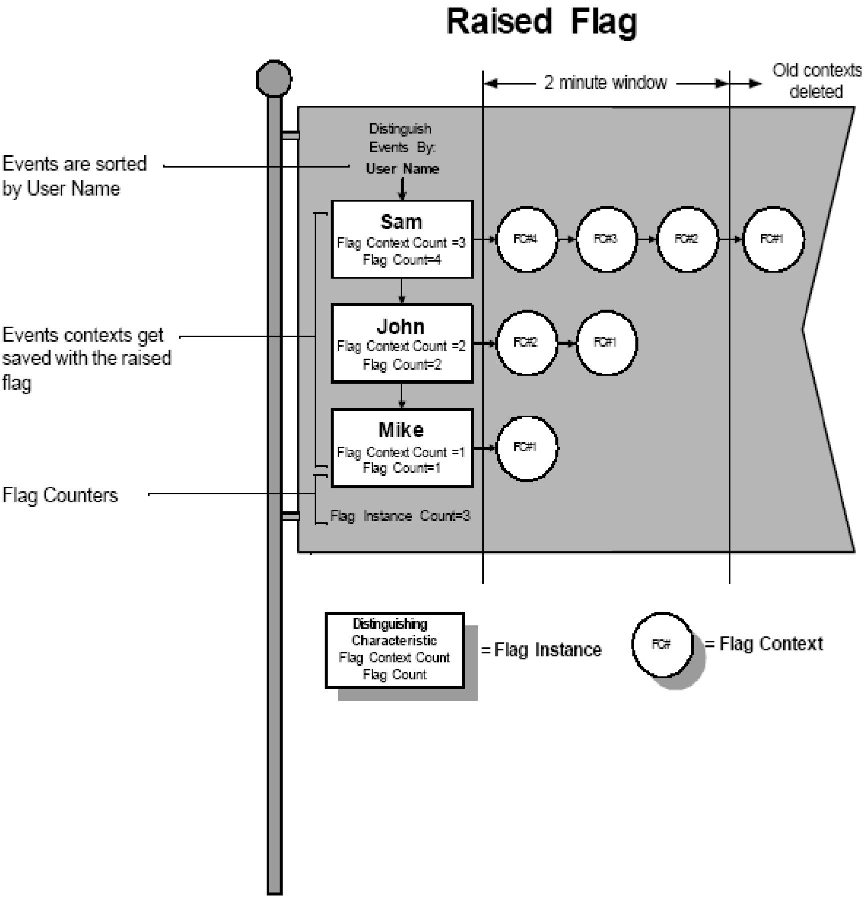


The policy states that among the many failed logins that occur, we want to identify the user that fails three or more logins within a two-minute period.

Now, let's take a closer look at the flag to better understand how event context capturing works.

The following graphic is used for illustrative purposes only; events stored with the flag cannot be seen or accessed by users.

Figure 10-3 Intruder Alert flag diagram



In the above diagram notice that the first failed login event raises the flag. Subsequent failed logins are stored with the flag for the period of time specified on the flag.

When an event has resided on the flag for the specified period of time, the Agent deletes the event context. In this example, the oldest event, Sam's first failed logon, gets deleted after two minutes.

As events accumulate on the flag, they are sorted by a user-defined event variable. In this example, events are sorted by user name. Each user has its own category. These categories are also called "Flag Instances." Intruder Alert allows you to select the criterion by which events will be categorized.

Using the proper selection criteria, you can determine when flag and event context conditions should trigger an action. In the next section, you will learn how to define that selection criteria.

Event context selection criteria

The Select/Ignore Flag selection criteria is defined using event variables in logical statements. In this section, you will learn how to build these statements to select the desired events.

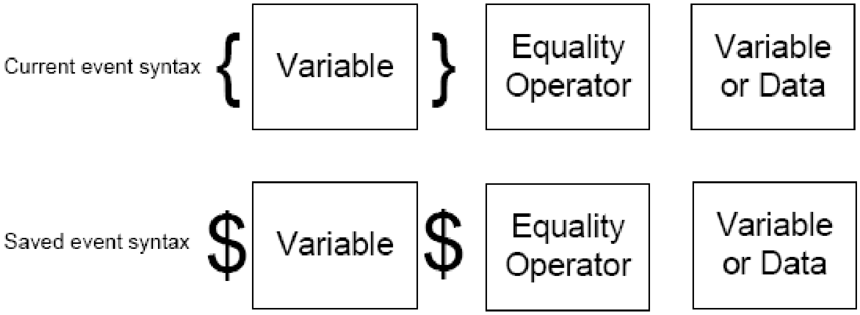
More specifically, you will learn:

- The select statement syntax
- The available event variables
- The available flag count variables

Select statement syntax

Select statements must use the following syntax.

Figure 10-4 Select statement syntax



The brace ({}) and dollar symbols ($) are used as variable delimiters. Intruder Alert differentiates between events saved on the raised flag (the "saved" events) and the event currently being evaluated by the Agent. The braces ({}) are used to specify the current event and the dollar symbol ($) is used to specify the saved events.

Table 10-1 describes the supported Select statement equality operators.

Table 10-1 Select statement equality operators

Operator	Name	Description
=	Equal To	Selects events in which the event variable contains the specified variable or text.
!=	Not Equal To	Selects all events except those in which the event variable contains the specified variable or text.
<	Less Than	Selects events in which the event variable contains a value lower than the stated value.
>	Greater Than	Selects events in which the event variable contains a value greater than the stated value.
<=	Less Than Or Equal To	Selects events in which the event variable contains a value less than or equal to the stated value.
>=	Greater Than Or Equal To	Selects events in which the event variable contains a value greater than or equal to the stated value.

The data portion of the Select statement may list another variable or specific text.

The following are examples of valid Select statements:

- {User Name} != Courtney
- {Flag Context Count} >= 5
- {Minute} =$ Minute$
- $Process ID $= 1145370

Note: The Select/Ignore Flag supports multiple Select statements. The relationship between multiple statements is determined by the And/Or radio buttons located near the rule's Label field.

Event variables

Event variables can be selected with the Raise Flag action only.

The following table lists the event variables supported in Intruder Alert.

Table 10-2 Event variables

Variable	Type	Current / Saved	Description
User Name	String	Saved only	The name of the user that generated the event. For example: {User Name}= jdoe
Process ID	Numeric	Saved only	The name of the process that generated the event. For example: {Process ID}= 517
Year	Numeric	Both	The year in which the event occurs. For example: {Year}=2001
Month	Numeric	Both	The numeric month in which the event occurs. Valid values range between 1 and 12. For example, to select events in the month of July, type: {Month}=7
Day	Numeric	Both	The day of the month in which the event occurs. Valid values range between 1 and 31. For example: {Day}>15
Hour	Numeric	Both	The hour in which the event occurs. Valid values range between 0 and 23. For example: {Hour} >= 18
Minute	Numeric	Both	The minute in which the event occurs. Valid values range between 0 and 59. For example: {Minute} >= 30

Flag count variables

Flag count variables or flag counters, are variables that count event occurrences during the lifetime of the flag. Flag count variables allow you to trigger an action when a certain number of events have occurred.

Flag count variables are used with the Select Flag option.

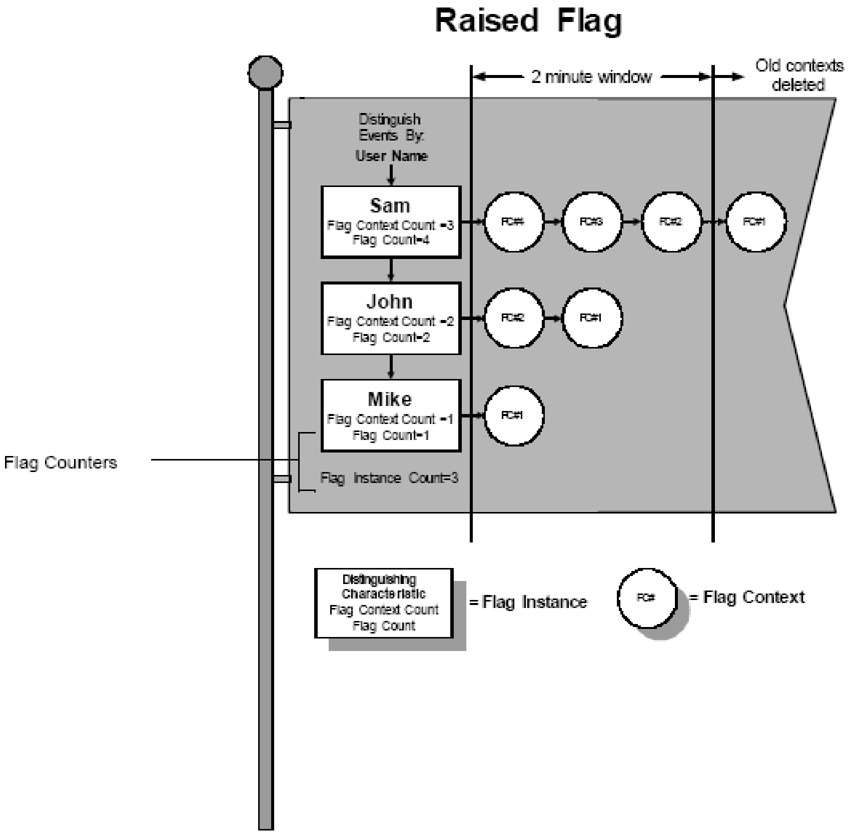
There are three flag counters.

- Flag Instance Count
- Flag Count
- Flag Context Count

To understand the difference between these variables, return to the example where Sam, John, and Mike caused seven failed logins within a two-minute period.

In the following diagram, note the three flag counters and how they are used.

Figure 10-5 Flag counter diagram



The following sections describe each variable in more detail.

Flag Instance Count

The Flag Instance Count variable refers to the number of unique instances created during the flag's lifetime. When an event is saved with a flag, it is sorted by a user-defined criterion in the Raise Flag action. For example, if User Name is the criterion, the Flag Instance Count increments each time a new user name is created.

Use this counter to select when a certain number of instances have occurred. For example, you can select when five different users have caused the same event within a given period of time. The rule's select statement would read:

{Flag Instance Count} >= 5

Flag Count

The Flag Count variable refers to the number of event contexts associated with a flag instance during the flag's lifetime.

Use this variable when similar events occur numerous times within a given period of time. This counter places emphasis on the number of similar events rather than the amount of time in which they occur (compare with Flag Context Count, below). For example, this flag can be used to select four failed logins from the same user within a two-minute period. The rule's select statement would read:

{Flag Count} >= 4

In this example, the flag will execute when the same or similar event has occurred 4 times during the flag's lifetime.

Flag Context Count

The Flag Context Count variable refers to the number of events currently saved with a flag category. Events saved on a flag instance expire after they have lived for the period of time configured on the raised flag. More recent events will maintain the existence of the raised flag.

When an event's time to live has expired, the event is deleted, but the Flag Context Count remembers that the event occurred during the lifetime of the flag. In contrast with the Flag Count variable, this counter places emphasis on the time frame during which a number of events occur. In other words, it is significant that they occurred within the given period of time.

Use the Flag Context Count variable when it is important that a certain number of events occur within a given period of time. Thus, our example of detecting three failed logins by the same user within a two-minute period would use this counter.

For example,

{Flag Context Count} >= 3

Notes and known issues

- Intruder Alert is limited by the collection systems on which it resides. If the event collector provides the information, Intruder Alert can use it. The collector on Windows does not provide the user name of the person who generated a failed logon. All events are given the user name "System," which is the process that generated the event, not the actual user.
- Certain variants of UNIX, generate only one failed login message for every three failed attempts. Other varieties of UNIX generate an event message for

every failed login. Thus, you will need to adjust your selection criteria accordingly. Furthermore, you will need to activate the policy on only those systems for which it was designed to work.

- For the Intruder Alert Agent service to interact with the Windows desktop, you must configure Control Panel > Services for the Intruder Alert Agent.
  See "Configuring Agent service properties" on page 61.

Creating policies that use event context capturing

For event context capturing to work, there must be a minimum of two rules. The first rule selects the desired events and stores all or part of the event information on the raised flag. The second rule selects when conditions on the raised flag exist. It is also configured to perform another type of action, such as email an administrator. This section describes how to configure the first rule.

Configuring the Raise Flag action to use event context capturing

Note: Global flags cannot be set at the same time as the Save Events with Flag feature. To trigger global flags from the same selection criteria, add two Raise Flag actions to the same rule. Configure one to raise global flags and the other to save events.

To configure the Raise Flag action to save events

1. Do one of the following:
   - Create a new policy.
   - Open an existing policy.

   See "Creating a policy" on page 138.
2. Do one of the following:
   - Create a new rule.
   - Expand an existing rule.

   See "Adding and deleting a rule" on page 139.
3. Create the desired Select and Ignore criteria (such as failed or unsuccessful login).
   See "Adding and deleting rule criteria" on page 140.
4. Add a Raise Flag action.
   The Raise Flag configuration screen appears in the right pane.
5. In the right pane, check **Save Event Environment with Flag**.

6 In the Tag drop-down list, select the criteria by which saved events will be sorted.

7 Optionally, under Flag Lifetime, check **Flag has a Lifetime**.

8 If you checked **Flag has a Lifetime**, in the Days, Hours, Minutes, and Seconds boxes, configure the duration of the flag.

Intruder Alert will raise the flag for the period of time defined in the time configuration fields.

9 Optionally, to have the flag lifetime reset with each new trigger, check **Reset Flag Lifetime with Each Trigger**.

Each new trigger will reset the flag lifetime to the time specified in the time configuration fields.

10 In the Intruder Alert tree, right-click the policy name, and click **Save** in the drop-down list.

You can create another rule to select or ignore the events captured by the raised flag.

See "Configuring Select/Ignore Flag to use event context capturing" on page 166.

Configuring Select/Ignore Flag to use event context capturing

This section describes how to configure Select Flag and Ignore Flag to use event context capturing.

Note: The Select/Ignore Flag and the Raise Flag action cannot reside in the same rule. They must reside in separate rules.

To configure the Select Flag

1 Complete the steps for configuring the Raise Flag action to capture event context information.

See "Configuring the Raise Flag action to use event context capturing" on page 165.

2 In the Intruder Alert tree, in the desired policy branch, create a new rule and name it.

See "Adding and deleting a rule" on page 139.

3 In the tree, under the new rule, click **Select** to display the Select toolbar above the right pane.

4 In the Select toolbar, click **Select Flag**.

5. In the right pane, drag the raised flag from the Available box and drop it in the Flags to Monitor box.
6. Double-click the flag's icon in the Flags to Monitor box.
7. In the Select Flag Criteria dialog box, in the edit box, type the desired select statement or statements.

   Each statement must reside on its own line in the edit box. The relationship each statement has to the others is determined by the And and Or radio buttons located near the Select criteria's Label field.

   See "Select statement syntax" on page 159.
8. When you have finished defining the desired select statements, click **OK**.

   The changes are automatically saved.
9. Optionally, add and configure the desired Ignore criteria and action using the procedure below.
10. Activate and test the policy to ensure that it is working as desired.

To configure the Ignore Flag

1. Complete the steps for configuring the Raise Flag action to capture event context information.

   See "Configuring the Raise Flag action to use event context capturing" on page 165.
2. In the Intruder Alert tree, in the desired policy branch, create a new rule and name it.

   See "Adding and deleting a rule" on page 139.
3. In the tree, under the new rule, click Ignore to display the Ignore toolbar above the right pane.
4. In the Ignore toolbar, click **Ignore Flag**.
5. In the right pane, drag the raised flag from the Available box and drop it in the Flags to Monitor box.
6. Double-click the flag's icon in the Flags to Monitor box.
7. In the Ignore Flag Criteria dialog box, in the edit box, type the desired ignore statement or statements.

   Each statement must reside on its own line in the edit box. The relationship each statement has to the others is determined by the And and Or radio buttons located near the Ignore criteria's Label field.

   See "Select statement syntax" on page 159.
8. When you have finished defining the desired ignore statements, click **OK**.

   The changes are automatically saved.

9 Optionally, add and configure the desired Select criteria and action.

10 Activate and test the policy to ensure that it is working as desired.

Detecting four failed logins by the same user

Failed logins occur all the time. In fact, one or two failed logins by the same user is common. However, several failed logins by the same user may indicate an intruder attempting to gain unauthorized access to a system's resources.

To illustrate event context capturing, in this section we will build an Intruder Alert policy that detects four failed logins by the same user within a two-minute period.

This policy is designed for a UNIX system equipped with btmp event logging, such as HP-UX or Solaris. To simulate this event, we will use a telnet client to login to the UNIX host remotely.

To create the 4 Failed Logins policy

1 Start Intruder Alert Administrator, connect to a Manager, and expand the branch for that Manager.

2 In the tree, under the connected Manager, right-click **Policies** and then click **New** in the drop-down list.

3 In the right pane, in the Label text box, type the name of the policy as:
`4 Failed Logins`

4 In the Description text box, type:
`Detects 4 failed logins by the same user within a 2 minute period on UNIX systems.`

5 In the tree, expand the new policy.
The Applied Domains and Rules branches are visible.

6 In the tree, right-click **Rules** and then click **New** in the drop-down list.
A new rule is added as New Rule.

7 In the right pane, in the Label text box, type the following name for the rule:
`Rule 1`

8 In the tree, click **New Rule** to update the name.

9 In the tree, expand **Rule 1**.

10 In the Rule 1 branch, right-click **Select** and then click **New > System Message** in the drop-down list.

11 In the right pane, in the New Entry text box, type the message the Agent sends to the Manager and then click **Add to List**.
Example responses include:

```
Unsuccessful login
Repeated Login Failures on
```

12 In the tree, under Rule 1, right-click **Actions** and then click **New > Raise Flag** in the drop-down list.

13 In the right pane, in the Label text box, type:

```
User Name Flag
```

14 Check **Save Event Environment with Flag**.

15 In the Tag drop-down list, click **User Name**.

16 Check **Flag has a Lifetime**.

17 Set the Minutes to 2.

18 In the tree, to add a second new rule, right-click **Rules** and then click **New** in the drop-down list.

19 In the right pane, in the Label text box, type the following name for the rule:

```
Rule 2
```

20 In the tree, click **New Rule** to update the name.

21 Expand **Rule 2**, right-click **Select** and then click **New > Flag** in the drop-down list.

22 In the right pane, in the Label text box, type:

```
4 Failed Logins Flag
```

23 Drag **User Name Flag** from the Available box to the Flags to Monitor box.

24 Double-click **User Name Flag**.

25 In the Select Flag Criteria dialog box, in the edit box, type the following select statement and then click **OK**:

```
{Flag Context Count} >= 4
```

Be sure to include spaces between Flag, Context, and Count, and around the equality operator.

26 In the tree, under Rule 2, right-click **Actions** and then click **New > Record to Event Viewer** in the drop-down list.

There is no need to configure this action with additional text to record.

27 In the tree, right-click **4 Failed Logins** and then click **Save** in the drop-down list.

28 Right-click **4 Failed Logins** again and then click **Apply to Domain** in the drop-down list.

29 In the Apply Policy to Domain(s) dialog box, select the domain in which the target UNIX system resides and then click **OK**.

30 Complete the steps below for triggering the 4 Failed Logins event.

To trigger the 4 Failed Logins event

1. Start the telnet client software.
2. Specify the target telnet server.
   This server should be in the domain to which the 4 Failed Logins policy is applied.
3. When prompted for the Login and Password, enter pseudo values and then press **Enter**.
   The pseudo values will reflect different user names with phony passwords. Be sure to use the same user name at least four times, as well as trying other user names.
4. Repeat Step 3 three more times within a two-minute period.
   The 4 Failed Logins event should appear in the Manager's event database and in Intruder Alert Event Viewer. See the instructions below for viewing the event in Intruder Alert Event Viewer.
5. If the events do not display in the Event Viewer, add the Record to Event Viewer action to each rule of the policy, as a troubleshooting measure. After adding the Record to Event Viewer action to each rule of the policy, repeat steps 3 and 4 and watch the Event Viewer to confirm that each rule is working.

To view the event results in Intruder Alert Event Viewer

1. Start Intruder Alert Event Viewer.
2. Click **File > New Query**.
3. In the Query Builder window, do one of the following:
   - In the Manager box, select a Manager.
   - Type the name of a Manager and then press **Enter**.
4. In the Connect to Manager dialog box, specify a Manager, enter its User Name and Password and then click **OK**.
5. In the Query Builder screen one, click **Next**.
6. In the Query Builder screen two, click **Next**.
7. In the Query Builder screen three, in the Manager Objects box, expand **Policies**.
   The 4 Failed Logins policy should be visible.
8. Drag the 4 Failed Logins policy from the Manager Objects box to the Query List box and then click **GO!**.
9. The text view appears with the 4 Failed Logins event.

If the event does not appear in the text view, verify that the policy was configured properly and that it resides on the targeted Agent system. Repeat the steps for triggering and viewing the event.

Section 4

Monitoring events

This section discusses the following:

- Chapter 11: Using Intruder Alert Event Viewer
- Chapter 12: Generating and viewing reports

Chapter 11

Using Intruder Alert Event Viewer

This chapter includes the following topics:

Launching Intruder Alert Event Viewer

Intruder Alert Event Viewer is a graphical user interface used to query and view events or attacks captured by Agents. Intruder Alert Event Viewer gathers its data from events recorded by Agents in the event database located on a Manager system.

Intruder Alert Event Viewer has advanced data filtering capabilities, allowing you to select and display specific data of interest in several formats, including:

- Bar chart
- Line graph
- Pie chart
- Text view
- Report view

Intruder Alert Event Viewer runs on Windows operating systems. Managers and Agents should be installed and running prior to running Intruder Alert Event Viewer, and policies should be applied.

To launch Intruder Alert Event Viewer

- From the Windows Start menu, click **Programs > Symantec > Intruder Alert > ITA Event Viewer**.

  The Intruder Alert Event Viewer launch screen appears.

  You can create a new view, open a predefined view, or send an Intruder Alert command to an Agent system.

Using the Query Builder wizard

The Query Builder wizard guides you through the process of defining a query and generating a view. The wizard presents three consecutive screens. This section describes the elements in each screen, and how to use the Query Builder wizard to select and view desired events.

See the following sections for information about the wizard:

- Query Builder wizard screen one
- Query Builder wizard screen two
- Query Builder wizard screen three

A view allows you to see events that have occurred, or are occurring, on your enterprise. Intruder Alert Event Viewer also allows you to filter these events by selecting one or more of the following criteria:

- Agents
- User
- Policies
- Rules
- Rule value
- Date
- Time
- Specified text

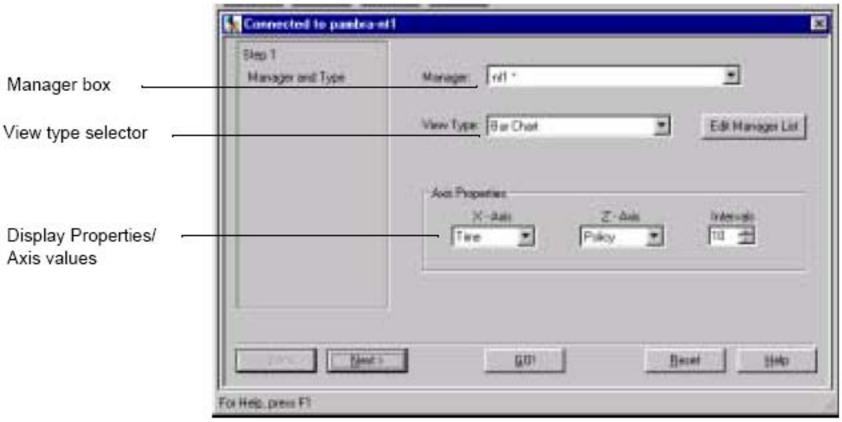
Note: Intruder Alert Event Viewer allows you to create multiple views, and have them open at the same time. This is useful for monitoring activity concurrently across multiple managers.

Query Builder wizard screen one

Access the Query Builder wizard from the Intruder Alert Event Viewer menu bar or toolbar by starting a new query.

See “Working in the Event Viewer” on page 185.

Figure 11-1 Query Builder wizard screen one



Manager: nt1 *

View Type: Bar Chart

X-Axis: Time

Z-Axis: Policy

Intervals: 10

The following sections describe the fields in screen one of the Query Builder wizard.

Manager box

Intruder Alert Event Viewer gathers data from a specific Manager, and only one Manager at a time may be selected. The Manager drop-down list allows the user to specify the Manager from which to gather data. The first time a user attempts to use the Event Viewer, the list will be empty.

After the first connection, Intruder Alert Event Viewer stores the name of the Manager in the drop-down list. If the Manager’s name does not appear in the list, type it in, and press Tab or Enter. The Intruder Alert Connect dialog appears.

See “Connecting to a Manager” on page 64.

View Type

Intruder Alert Event Viewer offers the following view types:

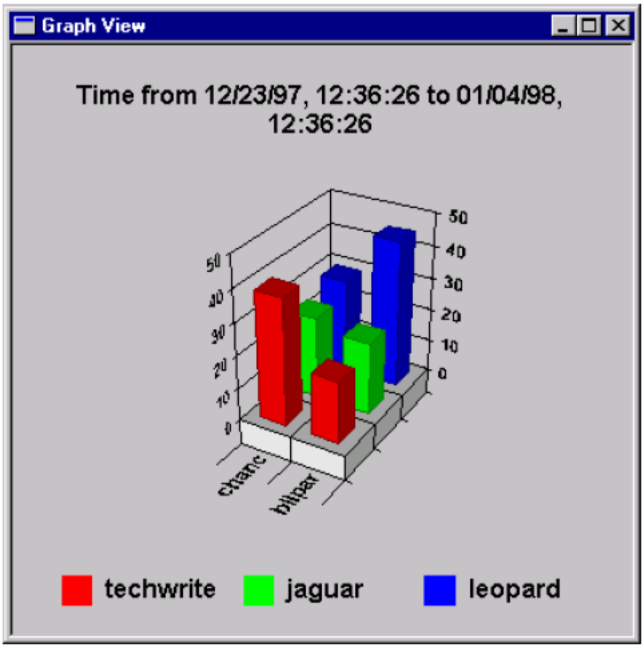
- Bar chart
- Line graph

- Pie chart
- Report view
- Text view

Bar chart

The following graphic illustrates the Intruder Alert Event Viewer bar chart.

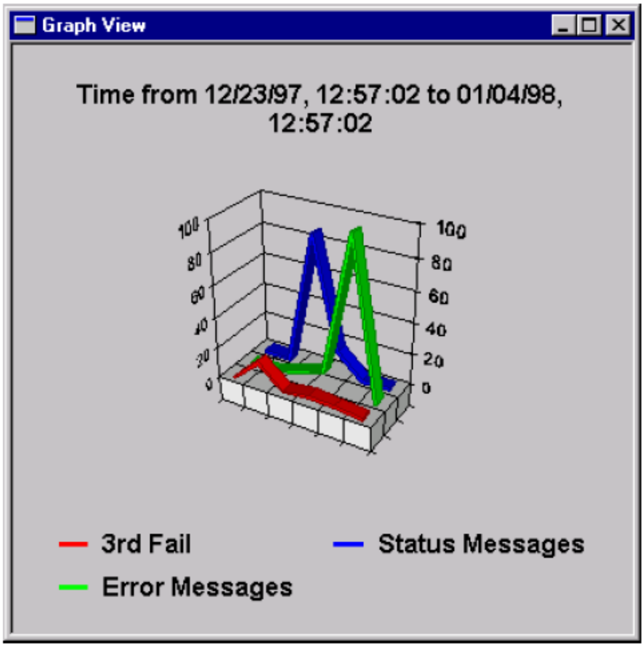
Figure 11-2 Bar chart view



Line graph

The line graph depicts the same data as the bar chart except that the data points are connected in a linear format. The following graphic illustrates the Intruder Alert Event Viewer line graph.

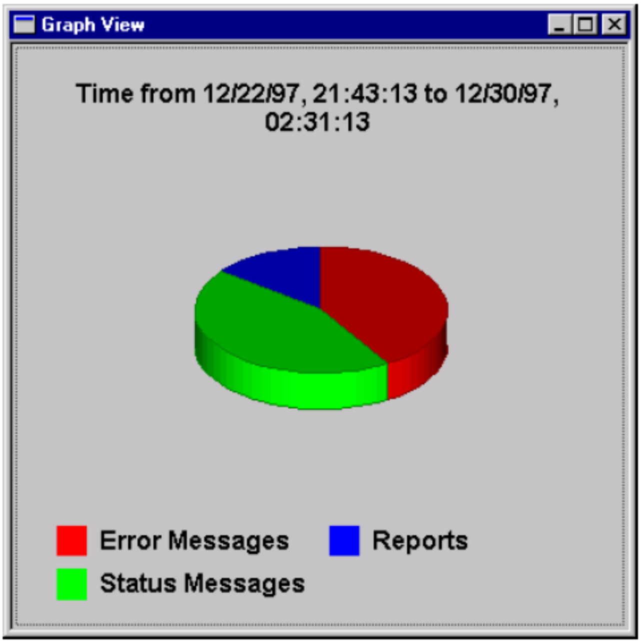
Figure 11-3 Line graph view



Pie chart

Select the pie chart view when you want to see what percentage each event contributes to the whole. The following graphic illustrates the Intruder Alert Event Viewer pie chart.

Figure 11-4 Pie chart view



Choose the category for the pie chart in the X Axis drop-down list.

Report view

The report view type displays event data in a Crystal Report viewing window.

When you select this option, you will be prompted to select a predefined report template. The report template defines what data to include in the report and how to format it. Intruder Alert Event Viewer comes with five predefined templates. In addition, if you have Crystal Reports, you can define your own custom templates and use them instead.

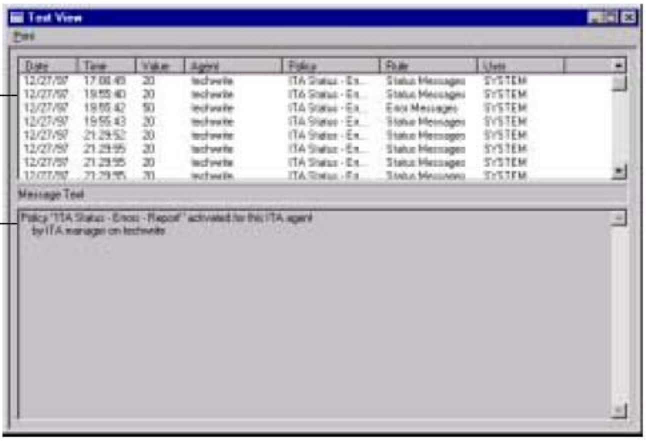
See “Generating and viewing reports” on page 199.

Text view

The text view shows the types of events being gathered. It is useful for verifying what events make up the bar chart, line graph, and pie chart views.

The text view screen has a top half and a bottom half. The top half of the view displays the policy rules that have triggered. The bottom half of the view depicts the actual event message and any defined labels added via the Record to Intruder Alert Event Viewer action clause or parsed event message data.

Figure 11-5 Text view



Date	Time	Value	Agent	Policy	Rule	User
12/27/97	17:08:49	20	techwrite	ITA Status - Ex...	Status Messages	SYSTEM
12/27/97	19:55:40	20	techwrite	ITA Status - Ex...	Status Messages	SYSTEM
12/27/97	19:55:42	50	techwrite	ITA Status - Ex...	Error Messages	SYSTEM
12/27/97	19:55:43	20	techwrite	ITA Status - Ex...	Status Messages	SYSTEM
12/27/97	21:29:52	20	techwrite	ITA Status - Ex...	Status Messages	SYSTEM
12/27/97	21:29:55	20	techwrite	ITA Status - Ex...	Status Messages	SYSTEM
12/27/97	21:29:55	20	techwrite	ITA Status - Ex...	Status Messages	SYSTEM
12/27/97	21:29:55	20	techwrite	ITA Status - Ex...	Status Messages	SYSTEM

```
Policy "ITA Status - Errors - Report" activated for this ITA agent
  by ITA manager on techwrite
```

You can resize the Message Text window to see additional event information or more text as desired. This is good for viewing several open text views at one time.

For more information about adding a text message event, see the section:

See "Record to Event Viewer" on page 106.

For more information about parsing event data, see the section:

See "Configuring external audit log monitoring" on page 85.

Axis properties

Variables are assigned to the axes on the bar chart, line graph, and pie chart view types. Available values on the X-Axis and the Z-Axis are as follows:

X-Axis	Z-Axis
Agent	Agent
Rule	Policy
Time	Rule
User	User
Value	Value

Intruder Alert Event Viewer allows you to define the values for both the X-Axis and Z-Axis of the bar chart and line graph. There is no Y-axis.

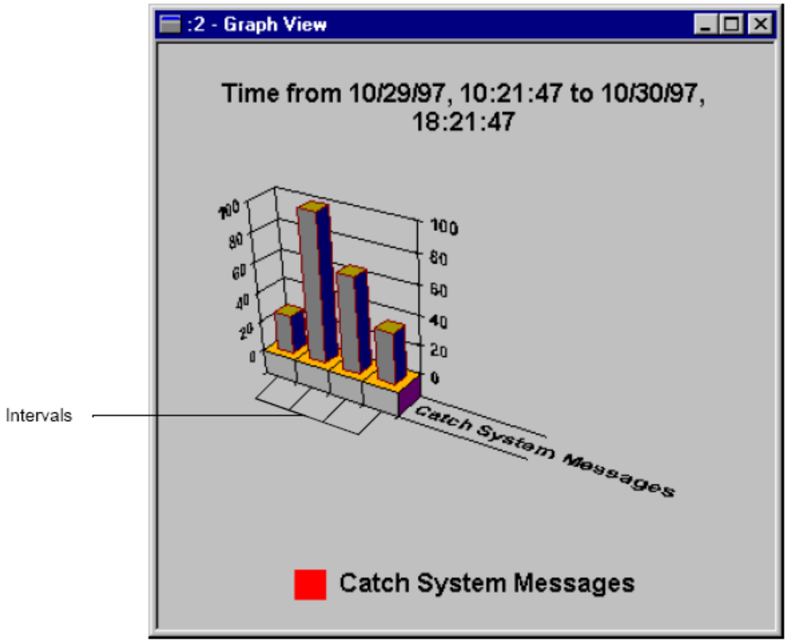
When defining a pie chart, X-Axis defines the category used for creating the pie.

Note: Axes are not used with the report or text views.

Intervals

Intervals refers to the number of divisions within a time period. The following graph illustrates the time intervals on a bar chart.

Figure 11-6 Time intervals

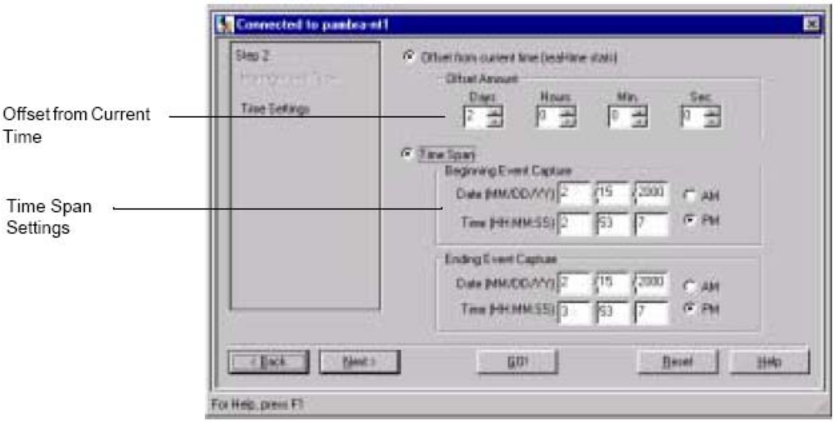


Query Builder wizard screen two

Access the Query Builder wizard from the Intruder Alert Event Viewer menu bar or toolbar.

See “Working in the Event Viewer” on page 185.

Figure 11-7 Query Builder wizard screen two



● Offset from current time (real-time stats)

Offset Amount

Days 2 Hours 0 Min. 0 Sec 0

● Time Span

Beginning Event Capture

Date (MM/DD/YY) 2 /15 /2000 ○ AM

Time (HH:MM:SS) 2 53 7 ● PM

Ending Event Capture

Date (MM/DD/YY) 2 /15 /2000 ○ AM

Time (HH:MM:SS) 3 53 7 ● PM

For Help, press F1

The following sections describe the fields in screen two of the Query Builder wizard.

Offset from Current Time (Real-Time Stats)

Intruder Alert Event Viewer allows you to specify how far back in time you want to view events. The default is to display events from the last two days.

Time Span

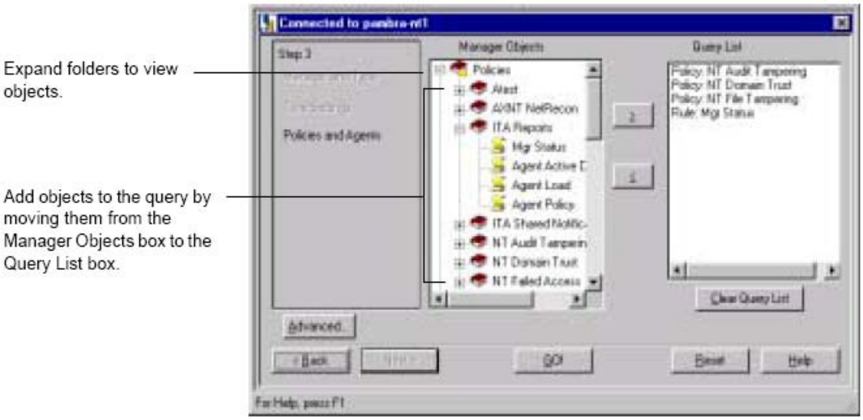
By selecting a starting and ending date and time, you can use the Time Span settings to frame an event window. The window would allow you to view events that occurred within a specified time parameter which does not necessarily include current events. This option is great for viewing historical events that may have been archived.

Query Builder wizard screen three

Access the Query Builder wizard from the Intruder Alert Event Viewer menu bar or toolbar.

See “Working in the Event Viewer” on page 185.

Figure 11-8 Query Builder wizard screen three



Policy: NT Audit Tampering
Policy: NT Domain Trust
Policy: NT File Tampering
Rule: Mgr Status

Expand folders to view objects.

Add objects to the query by moving them from the Manager Objects box to the Query List box.

The following sections describe the fields in screen three of the Query Builder wizard.

Manager Objects and Query List boxes

The Manager Objects box lists the policies, rules, and Agents you may select. To add an object to a query, drag it from the Manager Objects box and drop it in the Query List box.

The Query List box displays all policies, rules, and Agents on which the query will be generated.

If no items are selected, the default is to gather all events captured by the policies, rules, and Agents listed in the Manager Objects box.

Note: Limiting the number of selected objects to five or less will reduce complexity and make your reports and views easier to understand.

Advanced Query box

Clicking the Advanced button displays the Query text box in screen three. In the Query text box, you can define a query string that pinpoints specific data of interest. For example, you can direct Intruder Alert Event Viewer to display a specific type of event for a specific person.

There is a specific language and syntax used to define query strings.

See “Defining advanced queries” on page 192.

GO! button

This button is available at any stage of the Query Builder wizard, and can be used to launch the report based solely on the information that has been supplied to that point.

Working in the Event Viewer

This section provides instructions for performing the tasks available in Intruder Alert Event Viewer. These tasks include:

- Creating a new view
- Modifying a view's query definition
- Sorting the text view
- Loading a predefined view
- Modifying a chart view
- Saving a view
- Sending an Intruder Alert command to an Agent

Creating a new view

The steps below outline the process for creating a new view using the Query Builder wizard. If you need help using the Query Builder wizard, click Help or refer to the section:

See "Using the Query Builder wizard" on page 176.

To create a new view

1. Start Intruder Alert Event Viewer.
2. Click **File > New Query**.
3. In screen one of the Query Builder wizard, in the Managers box, do one of the following:
   - Type the name or IP address of the Manager
   - In the drop-down list, click the name or IP address of the Manager
4. In the Connect to Manager dialog box, enter the User Name and Password and then click **OK**.
   An asterisk (*) should appear next to the Manager's name in the Query Builder screen, indicating a successful connection.
   If the asterisk does not appear after a few seconds, the connection process was unsuccessful. Repeat the process avoiding any typographical errors. If

Intruder Alert Event Viewer still cannot connect to the Manager, make sure the Manager is installed and running.

You can use the nslookup command on the Manager's system to determine if the system is known to DNS. Also note that Intruder Alert Event Viewer and the Manager must be the same version.

5 In the Query Builder wizard screen, in the View Type drop-down list, click the desired view type.

Because the Report view type is significantly different than the other types of views, instructions for generating this type of view are discussed separately.

See Chapter 12, Generating and viewing reports.

6 Optionally, select the Axis and Interval settings and then click **Next**.

You are finished with the Query Builder wizard screen one.

7 In the Query Builder wizard screen two, do one of the following:

- To view events as they occur (data will be added to the view in real time), click **Offset from current time** (realtime stats) and define the offset amount.
- To view events that occurred within a period of time, click **Time Span** and then define the time span in the Beginning Event Capture and Ending Event Capture boxes.

8 Click **Next**.

You are finished with the Query Builder wizard screen two.

9 In the Query Builder wizard screen three, in the Manager Objects box, click the desired Manager objects and then click the right-arrow button to move them into the Query List box.

The query will be generated on the objects in the Query List box.

10 When you have finished defining the query, click **GO!**.

If you have defined a broad or complex query or if there is a large amount of data in the event database, it may take a few seconds longer to generate the view. In such cases, the message "Generating View" will appear. Wait for a few seconds until the view appears.

Modifying a view's query definition

After a view has been created, you can modify the query and recreate the view without entirely redefining the view.

To modify a view's query definition

1 If you have more than one view open, select the desired view.

2. On the menu bar, click **Edit > Query**.
   The Query Builder wizard appears with the current query settings defined.
3. Make the desired modifications to the query and then click **GO!**.
   Intruder Alert Event Viewer reads the event database on the selected Manager and recreates the view.

Sorting the text view

Sorting rearranges event records (rows) in the text view based on the selected criteria, such as date, time, and policy. You can sort rows by column heading in ascending (1 to 9, A to Z) or descending (9 to 1, Z to A) order.

To sort the text view

1. Create a text view.
2. In the text view, do one of the following:
   - To sort the text view in ascending order, click the desired column heading once.
   - To sort the text view in descending order, click the desired column heading twice.

Loading a predefined view

Intruder Alert Event Viewer allows you to save queries with or without Manager connection information. A query saved without Manager connection information is called a “generic view.” Generic files are saved with an .ivg file extension. Queries saved with Manager specific information are given a .ivw file extension. This section describes how to load both view types.

Note: You can save the view as a shortcut to the desktop. To activate, double-click on the shortcut icon.

To load a generic view

1. Click **File > Load Generic View**.
2. In the Open dialog box, click the desired view file and then click **Open**.
   If the Open dialog defaults to your desktop it will be necessary to drill down to the following file location:
   <system disk>:\Program Files\Symantec\ITA\bin
3. In the Connect to Manager dialog box, type a Manager’s name, User name, and Password into the corresponding fields and then click **OK**.

4 In the Query Builder screen, click **GO!** to generate the view using the generic view settings.

Depending on the amount of data in the event database, it may take a few seconds to generate the view. The message “Generating View” may appear. The view will appear after gathering the selected data.

There are no predefined .ivw files. Views with Manager information that are created and saved by users will default to the .ivw extension.

To load a regular view

1 Start Intruder Alert Event Viewer.

2 Click **File > Load View**.

3 In the Open dialog box, specify the desired view (.ivw) file and then click **Load**.

If you are not already connected to the Manager, the Connect to Manager dialog box appears with the name of the Manager, the user name, the protocol, and the service number already loaded.

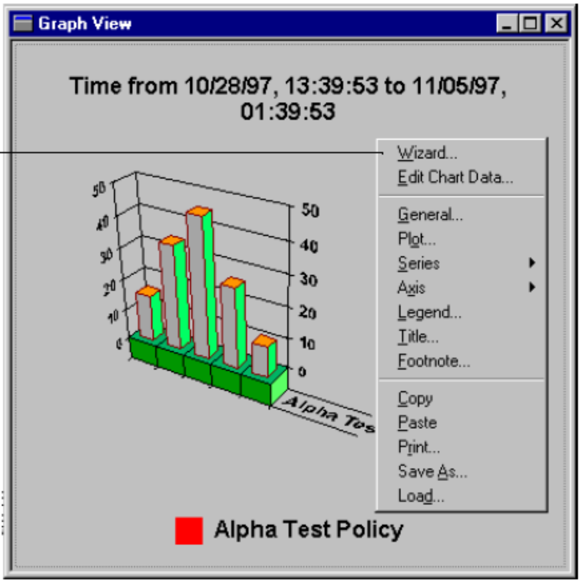
4 In the Connect to Manager dialog box, type the Password and then click **OK**.

Depending on the amount of data in the event database, it may take a few seconds to generate the view. The message “Generating View” may appear, The view will appear after gathering the selected data.

Modifying a chart view

After creating a chart view, you can modify the view’s appearance by right-clicking anywhere in the graph view screen and selecting an editing tool from the pop-up Graph Editing menu.

Figure 11-9 Graph Editing menu

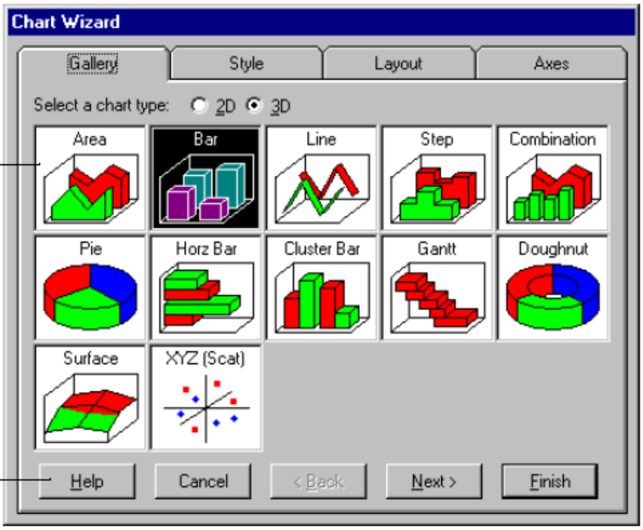


Right-click in this screen to access the Graph Editing Menu.

Use the tools on the Graph Editing menu to modify aspects of the chart.

For example, by clicking Wizard, the Chart Wizard appears. The Chart Wizard walks you through the process of modifying the chart's type, style, layout, and axis.

Figure 11-10 Chart Wizard



Select a chart type: ○ 2D ● 3D

Select an option and click Next until finished.

Click Help for online assistance.

Saving a view

After defining a query, you can save the view that is generated for future use. Saving a view saves you from having to redefine it each time you want to examine that the results of that query.

To save a view

1 If you do not already have a view open, create a view.
See “Creating a new view” on page 185.

2 In the Event Viewer menu bar, click **Edit > Query**.
This brings up the Query Builder wizard, and adds the save option to the available menus.

3 In the menu bar, click **File > Save View**.

4 In the Save As dialog box, specify a directory and file name and then click **Save**.
Save user-defined files with a .ivw file extension. Save modified generic views with a .ivg file extension.

Sending an Intruder Alert command to an Agent

The Send Intruder Alert Command feature allows you to send an Intruder Alert command to an Agent system from Event Viewer. This feature works in conjunction with an Intruder Alert command located in a policy activated on the Agent. Commands are user-defined and can be any alpha-numeric combination you wish.

The following are example commands:

- page administrator
- cancel timer

If you send the command "page administrator" to an Agent, a policy on the Agent system must have a Select Intruder Alert Command containing the words "page administrator."

In addition to sending user-defined commands, the Send Intruder Alert Command program has one hard-coded command called "report." The report command generates three reports containing information about the Agent.

See "Generate an Agent report" on page 213.

To send an Intruder Alert command to an Agent

1. Do one of the following:
    - On the Intruder Alert Event Viewer toolbar, click **Send Command**.
      This is the ITA! icon on the toolbar.
    - On the Event Viewer menu bar, click **ITA > Send Intruder Alert Command**.
2. In the Send ITA Command dialog box, in the Manager text box, do one of the following:
    - Type the name or IP address of the Manager
    - In the drop-down list, click the name or IP address of the Manager
3. In the Agent text box, do one of the following:
    - Type the name or IP address of the Agent
    - In the drop-down list, click the name or IP address of the Agent
4. In the Command text box, type the command.
   If the Case Sensitive check box is selected in the policy, the command is case sensitive, so use the exact case when specifying a command.
5. Click **Send Command**.
6. Optionally, to send a command to another Agent on a different Manager, click **New Manager**.

7 In the Connect to Manager dialog box, enter the connection criteria for the new Manager and then click **OK**. Then complete steps 3-5 above.

Defining advanced queries

In the Event Viewer, you can define advanced queries on screen three of the Query Builder wizard. This screen contains a button labeled Advanced.

Clicking the Advanced button displays the Query text box to the right of the button. In the Query text box you can define a query string to specify data of interest. For example, you can direct Intruder Alert View to display a specific type of event for a specific person. This section describes the query language and syntax used to define query strings.

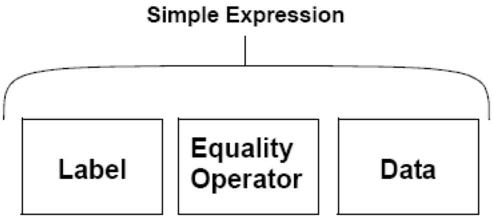
Section topics include:

- Building blocks of a query
- Building complex queries

Building blocks of a query

There are three basic building blocks of a query: label, equality operator, and data. The three together constitute a simple expression. See below.

Figure 11-11 Simple expressions



The following is an example of a simple expression.

User=Guest

This simple expression tells Intruder Alert View to collect and display only the data corresponding to the user “Guest.”

Users can combine simple expressions. More than one simple expression joined by a logical operator constitutes a compound or complex expression. Complex queries are discussed later in this chapter.

The sections below describe the fundamental building blocks of a simple expression and how to use them to build expressions or queries.

Labels

A label is the first element in a simple expression. Labels identify classes of information. The following table describes each label.

Table 11-1 Query labels

Label	Description
Value	Each rule has an associated value. The values range from 0 to 100, 0 being the least severe and 100 being the most severe. When Intruder Alert detects a security event, it stamps the event with additional data. One of those elements is the rule value. Thus, you can query the event database based on the rule value. Use this label when you want to include or exclude events having a particular rule value. For example, Value>=50
System	System refers to the name of the Agent on which the event was captured. This allows you to select or exclude events stemming from specific systems. For example, System=Spartan
Policy	Policy refers to the name of the policy that detected the event. Add policy names to the query or add policy names using the Manager Objects/Query List boxes. With either method, the results are the same. For example: policy!=NT User Changed
Rule (not available on UNIX)	Rule refers to the name of the rule that detected the event. Add rule names to the query or add rule names using the Manager Objects/ Query List boxes. With either method, the results are the same. For example: rule=Account-Changed
User	User refers to the user name of the person that generated the event. If, for example, on a UNIX system you have multiple users logged in at once, you can select events generated by specific users. For example: user=jdoe

Table 11-1 Query labels

Label	Description
TXT	The TXT (all in caps) label allows you to define specific text on which to query. This label can only be used with the equals (=) equality operator. For example: TXT=Source: Security

Note: Use the Offset fields (in screen two of the Query Builder wizard) to define the time period parameters.

Note: Labels created when parsing user-defined audit logs are also available for query definition.

Equality operators

Equality operators are used within simple expressions. (Logical operators, discussed under Complex Queries later in this chapter, are used between simple and complex expressions.) Intruder Alert View uses the following equality operators.

Table 11-2 Equality operators

Operator	Description
=	Equal to
!=	Not equal to
<	Less than
>	Greater than
<=	Less than or equal to
>=	Greater than or equal to

Examples include:

- User=jdoe
- Policy!=Collector
- Value>60

Note: Do not add spaces before or after the operator.

Data

The data element in a simple expression contains a specific instance of the label. The data element need not be surrounded by quotation marks unless a space or special character exists in the segment. For example,

rule=”Failed Logon”

The data element may also contain wildcard operators. Use the asterisk (*) wildcard character in place of multiple missing characters or words and the question mark (?) wildcard operator in place of single missing characters. For example,

system=acct*

Note: The data element is case-sensitive, allowing for more discriminating selection. Be deliberate when using upper and lower case to define the data segment.

Use the following guidelines when inputting the data element, Use quotes around multiple-word data elements, such as multiple-word policy and rule names.

Table 11-3 Data element guidelines

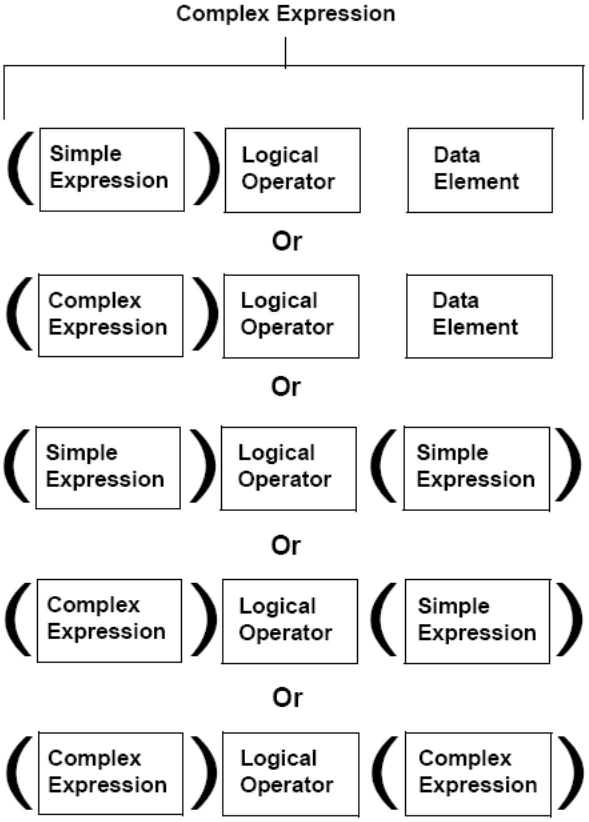
Label	Suggestion
Value	Value>50
System	System=Baddog
Policy	Policy=”NT User Account or NW Help Desk”
Rule	Rule=”Account Changed”
User	User=jdoe

TXT	Type specific text to query. Examples include:
	TXT=PID:*123456789
	TXT=”Failed Logon”

Building complex queries

Complex queries contain two or more simple expressions linked by a logical operator. Simple and complex expressions can be linked in various forms to make complex queries. Use parentheses to group expressions together. See the examples under Logical operators on the next page. The following illustration depicts the various forms of a complex query.

Figure 11-12 Complex expressions


Complex Expression
(Simple Expression) Logical Operator Data Element
Or
(Complex Expression) Logical Operator Data Element
Or
(Simple Expression) Logical Operator (Simple Expression)
Or
(Complex Expression) Logical Operator (Simple Expression)
Or
(Complex Expression) Logical Operator (Complex Expression)

Logical operators

Logical operators are used between simple and complex expressions. The actual operator must be used, NOT the value that it represents. Intruder Alert Event Viewer uses two logical operators.

Table 11-4 Logical operators

Operator	Description
& (Ampersand)	And Selects events that satisfy the criteria contained in both the expression on the left and the expression on the right. The event message must match both sets of criteria.
| (Pipe)	Or Selects events for the expression on the left or the expression on the right. Either expression will satisfy the selection criteria.

Examples include:

- (user=smitty)&(value>60)
- (policy!=”System Messages”)&(value>=50)

Note: The order of precedence is first, inside parentheses; and second, from left to right.

Generating and viewing reports

This chapter includes the following topics:

About reports

Intruder Alert’s report generator is designed to present information in a meaningful format. Reports offer a published look and feel and allow mixed content of text, charts, and graphs. With this tool, you can generate easy-to-read security reports tailored for different audiences.

Intruder Alert’s report generator allows you to use your own Crystal Reports templates to display security information in any format. You may export report data to other standard database formats, including CSV, TSV, XLS, WKS, RPT, and many more.

Security reports generated from Intruder Alert Event Viewer have the following reporting capabilities.

- Data export
  The product provides a feature that allows the user to define an export filter in Event Viewer, and export the matching data to an MS Access Database.

The export filter allows a user to select data for export based on event date and other data attributes. When data is exported into the default MS Access database, it is protected with the appropriate MS Access security features.

- Commercial report writer
  Users are able to modify the default report templates and design their own reports (provided they have purchased the tools separately). They are also able to run and view these reports from within the product environment.
  A set of pre-defined, easily modifiable reports have been included. Report media includes printable, electronic, HTML, RTF, and ASCII formats.
- Content
  Since the reports are one of the most visible elements of the product, pre-defined reports have undergone testing to verify the accuracy, relevancy, presentation, and usability of the product.
- Graphs and trends
  Charts provide a graphical trend-analysis that displays relative history, over a definable period of time, against a definable set of threats. Graphs are used for real-time reporting in control centers, and allow customization of graph properties like title, color, sticky-notes, etc.
- Selectable summary detail
  All reports and trend analysis are designed to report events in terms of the following selectable criteria:
  - Scope
  - Time window
  - Audience (management, technician):

Management:	This report is intended for senior management. It provides the highest level of summary information and the least amount of specific detail. It uses charts and graphs largely to communicate status measured in terms of company-wide business objectives.
Technician:	This report is intended for the systems administrator or security practitioner. It is a detailed report showing events on specific systems. The user may use this report to identify what precautions may be taken to eliminate risk.

  - Type of detail (security events, agents, or users):

Security events:	This report sorts data by event type across one or more systems.

Agents: This report sorts data by system and the events occurring on that system.

Users: This report sorts data by user, date, and severity level.

Integrating Crystal Reports

You must own a fully licensed version of Crystal Reports to take complete advantage of Crystal Report capabilities including the option to customize your report page with custom logos.

Crystal Report integration with Intruder Alert provides the following benefits:

- Choice of a variety of report types
  Choose from sub reports, conditional reports, summary reports, form reports, drill-down, OLAP, Top N, multiple detail reports, mailing labels, and more.
- Easy access to Intruder Alert event logs
  Connect to over 30 different types of OLAP, SQL, and PC databases including Microsoft SQL Server, Lotus Domino, and Oracle, using supported native ODBC connectivity.
- Ability to customize the look of your report
  Address complex reporting requirements with advanced features including grouping, sorting, sub reports, and cross-tabs.
  To learn more about Crystal Reports visit the following Web site:
  http://www.businessobjects.com/

Understanding security reports

The information in this section answers the following common questions about reports.

- Why generate reports?
- What reports are available out of the box?
- How do I create and use my own Crystal Reports templates?

Why generate reports?

Intruder Alert reports help you see:

- What attacks occurred on your enterprise
- Where those attacks occurred (i.e., the hosts on which they occurred)

- How many attacks occurred
- Who the attackers were

Having this information presented in a clear, concise format helps you prevent the misuse of information resources. With this information you can take preventative measures as necessary, including disabling a user's account, restricting file and directory access, and disabling vulnerable services.

Also, reports can be printed and distributed to management and technicians, or they can be exported and used in another application.

What reports are available out of the box?

Intruder Alert comes with six standard reports, described in the table below.

Table 12-1 Standard report types

Report	Description
Management Report	The Management Report targets business executives who may not have technical backgrounds or a lot of time. Use this report to give upper management an illustration of detected attacks by severity, Agent, and user. The Management report presents summary information using charts and graphs.
Technician Report	The Technician Report targets information security and system administrators. The Technician Report provides the greatest level of detail. Not only does it present information in tables and charts, but it also lists each attack by severity, Agent, or user. Use the Technician Report when you want to give security and system administrators a comprehensive view of detected attacks.
Security Events Report (Sorted by Severity)	The Security Events Report simply lists detected events in a report. The report is sorted by severity level first then Agent system in alphabetical order second. Use this report to get a list of all attacks matching the desired criteria.
Agent Report	The Agent Report views events from the Agent's point of view. It compares events on selected Agents, plus it reveals events detected for each user on the selected Agents. Use this report when you want to compare Agent systems and view user activity on each Agent. The Agent Report uses a default Crystal Reports template (AgentsReport.rpt) located in the ITA\bin directory.

Table 12-1 Standard report types

Report	Description
Security Report	The Security Report views events from a security point of view. It compares the severity of events by Agent, user, and date. In addition, it lists events by severity level. The Security Report uses a custom Crystal Reports template (SecurityReport.rpt) located in the ITA\bin directory.
User Report	The User Report views events from a user perspective. It compares the severity of event by user, users on an Agent, and date. In addition, it lists events sorted by user and severity level. The User Report uses a custom Crystal Reports template (UsersReport.rpt) located in the ITA\bin directory.

Reports are generated through the Query Builder wizard by selecting the Report view type and defining the parameters of the query as with any other view type.

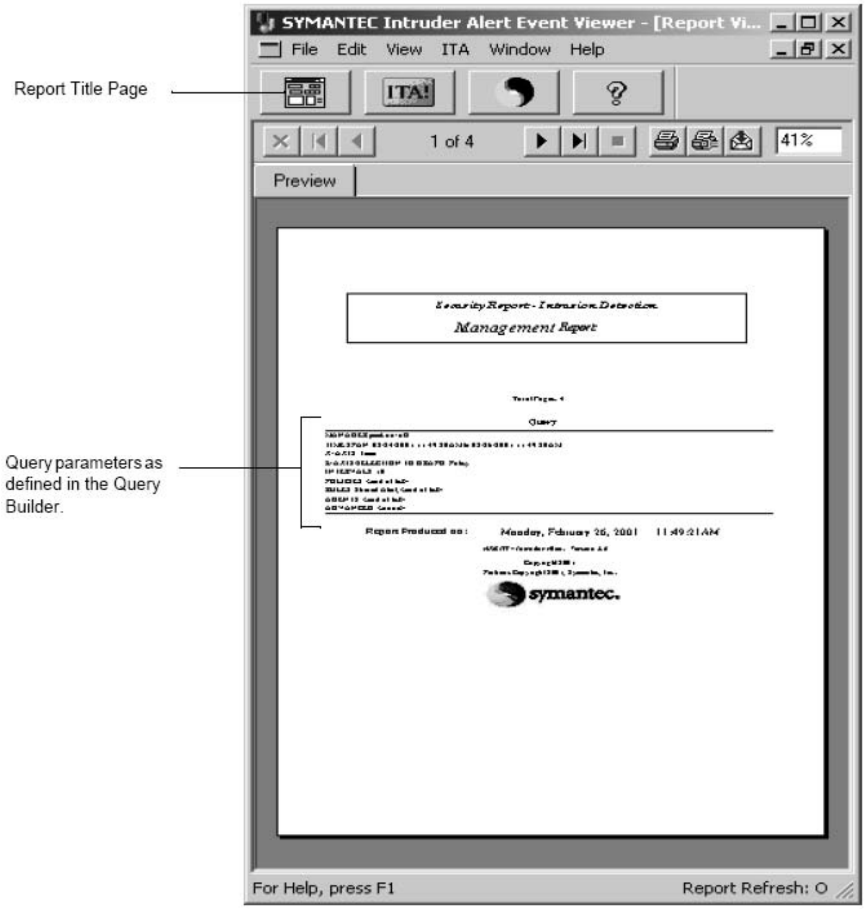
The Generate Report dialog box appears, allowing you to select the audience and level of detail for a comprehensive report. Or, you can select a Security Events Report that simply provides a list of all events matching the query definition sorted by level of severity. This report does not contain summary graphs or charts.

Alternatively, you can select a Custom Report that can use a Crystal Reports template for generating the report. Intruder Alert comes with three such templates, the Agent Report, Security Report, and User Report. These templates reside in the ITA\bin directory.

Under Custom Reports, you can also use your own custom report template. The dialog has a browse feature to allow you to select the template. User-defined report templates should be stored in the predefined ita\bin\Custom_Reports directory.

After making your selections, the report appears in the Report Viewer, as illustrated below.

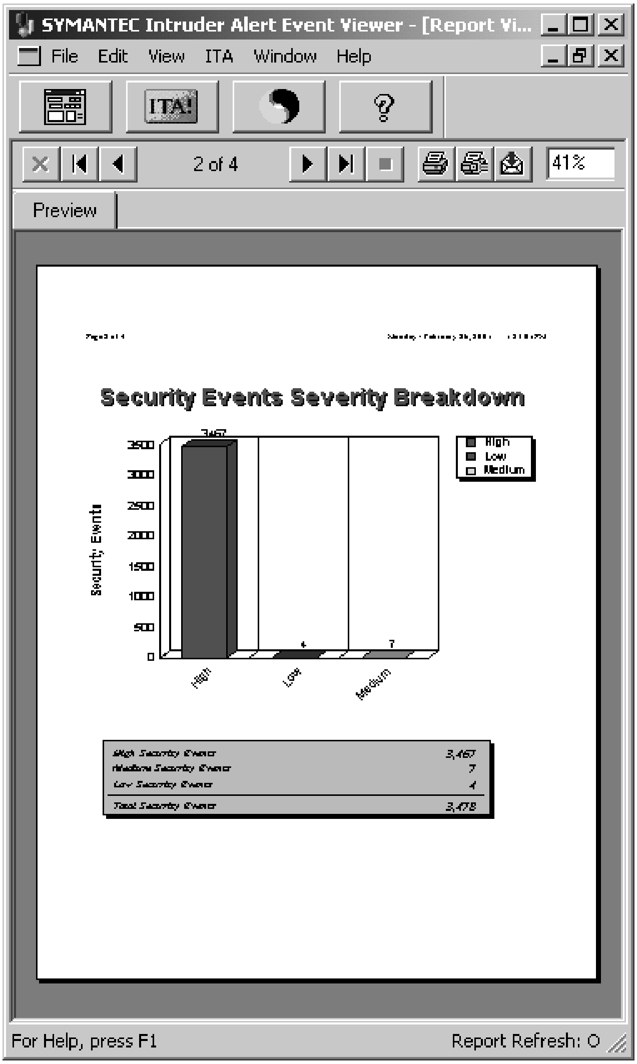
Figure 12-1 Report Viewer


Report Title Page
Query parameters as defined in the Query Builder.
SYMANTEC Intruder Alert Event Viewer - [Report Vi...
File Edit View ITA Window Help
ITA!
1 of 4
41%
Preview
Security Report - Intrusion Detection
Management Report
Query
Report Produced on : Monday, February 26, 2001 11:49:21 AM
symantec.
For Help, press F1
Report Refresh: 0

The body of the report contains various report elements such as, charts, graphs, and listings of individual events.

The following graphic illustrates the Security Events Severity Breakdown chart and graph.

Figure 12-2 Security Events Severity Breakdown chart



High Security Events	3,467
Medium Security Events	7
Low Security Events	4
Total Security Events	3,478

How do I create and use my own Crystal Reports templates?

Intruder Alert's report generation feature allows you to control how security information appears in a report. This is done using customized report templates created in Crystal Reports. Crystal Reports is a popular third-party report design and report generation tool. If your organization has specific reporting requirements, you will need to create your own template in Crystal Reports, and use that template in Intruder Alert.

To create a template in Crystal Reports, you will need:

- Database file in Microsoft Database (.mdb) format containing 100 to 200 events captured by Intruder Alert
- The database map or table definition.
  The table definition describes the type, location, and size of the various fields in the database.
- Fully licensed version of Microsoft Access

Note: For help with creating a Crystal Reports template, consult Crystal Reports' documentation and help.

To create a Microsoft Database (.mdb) file

1. Export a generated report from the Report Viewer in comma-delimited format. For instructions on how to export Intruder Alert data from the Report Viewer, see the section:
   See "Export and save the report contents" on page 210.
2. Import that data file into Microsoft Access.
3. Save or export the data in Microsoft Database (MDB) format.
   These events will be used to design the tables and charts in Crystal Reports' Report Designer.

The following table describes the events database. Use this information when creating the report template in Crystal Reports.

Table 12-2 Database definition table

Field	Type	Size	Notes
Date	Text	13	
Time	Text	13	
Value	Text	13	
System	Text	255	Must be static size of 255 for queries, sorts, and indexing. System can be 256.
Policy	Text	35	
Rule	Text	35	
User	Text	35	

Table 12-2 Database definition table

Field	Type	Size	Notes
Event Text	Memo	256+	

Generating security reports

To generate a security report

1. Open the Event Viewer
2. Click **File > New Query**.
3. In Screen One of the Query Builder wizard, in the Managers box, do one of the following:
   - Type the name or IP address of the Manager
   - In the drop-down list, click the name or IP address of the Manager
4. If the Event Viewer is not connected to the selected Manager, the Connect to Manager dialog box appears. In this case, you must connect to the Manager before continuing.
   See "Connecting to a Manager" on page 64.
5. In the View Type box, click **Report** and then click **Next**.
6. In Screen Two, set desired time parameters and then click **Next**.
7. In Screen Three, select the desired Manager Objects and set any advanced query strings and then click **GO!**.
   For more information about how to generate reports and set query parameters, see the section:
   See "Creating a new view" on page 185.
8. In the Generate Report dialog box, in the Report Title text box, optionally type a title for the report.
9. Do one of the following:
   - Under Standard Reports, click **Audience/Detail** and click a choice under Audience and under Detail.
     The Audience setting indicates for whom the report is intended, and the Detail setting indicates the type of information in the report.
   - Under Standard Reports, click **Generic Listing of Security Events** to get a list of all events matching the query definition sorted by level of severity.
     This report does not contain summary graphs or charts.

- Under Custom Reports, click **Custom Report Template** and click **Browse** to select a report in the custom reports directory.

  Intruder Alert comes with three Crystal Reports templates, the Agent Report, Security Report, and User Report. These templates reside in the directory:

  ```
  ita\bin
  ```

  User-defined report templates are stored in the predefined directory:

  ```
  ita\bin\Custom_Reports
  ```

10 Click **OK**.

If you selected an option under Standard Reports, the report is generated and displayed in the Report Viewer screen.

If you selected an option under Custom Report Template, the Select Report to View dialog box appears.

11 In the Select Report to View dialog box, select the path and file name of the desired report template and then click **Open**.

This dialog is used to select the desired Crystal Reports template.

The report is generated in the Intruder Alert Report Viewer window. This window is a Crystal Reports viewing screen.

If you have defined a general or complex query, or if there is a large amount of data in the event database, it may take a little longer to generate the report. In such cases, the message “Generating Report” will appear. Wait for the report to appear.

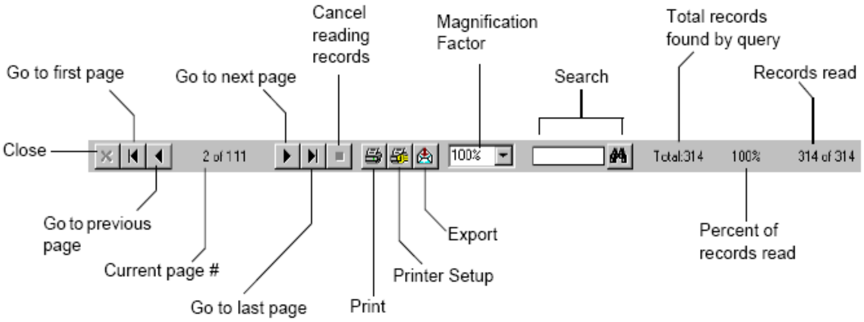
In the Report Viewer, you can print the report, export the report contents, and save the report.

Using the Intruder Alert Report Viewer

The Report Viewer is a Windows graphical interface used to display Crystal Reports templates.

The following graphic depicts the Report Viewer toolbar.

Figure 12-3 Report Viewer toolbar



This section describes how to use the Report Viewer. Section topics include:

- Refresh the report contents
- Suspend and resume automatic refresh
- Set up the printer
- Print the report
- Export and save the report contents
- Enlarge the view area
- Locate information in a report
- Exit the report

Refresh the report contents

Use the refresh feature to verify that the report contains the most recent events.

To update the report contents

1 In the Event Viewer, the desired Report View window must be active.

2 Click **Edit > Refresh Report**.
The report is updated with the latest events.

Note: Reports that include current information only need to be updated if you select the time setting, Time Span, in the query. If you select Offset from current time (real time stats) the report will automatically refresh.

Suspend and resume automatic refresh

In Offset From Current Time (real time stats) mode, the report view automatically refreshes itself in real time, meaning that events get posted on the report immediately after they occur. The Suspend Automatic Refresh feature allows you to disable Intruder Alert Event Viewer’s real-time updating temporarily.

If you have multiple report views open, the Suspend Automatic Refresh feature will suspend all automatic refreshing on all reports and views.

To suspend and resume automatic refreshing

1. Click **Edit > Suspend Refresh**.
   The automatic refresh function is suspended.
2. Click **Edit > Resume Refresh**.
   Automatic refreshing is resumed. If events occurred while automatic refreshing on all open report views was suspended, Intruder Alert View will update the open views with those events (this may take a few seconds).

Set up the printer

To set up the printer

1. On the Report View toolbar, click **Printer Setup**.
2. Select the desired printer, paper, and orientation settings.
3. Click **OK**.

Print the report

To print the report

1. Generate/open a report.
2. On the Report Viewer toolbar, click **Print**.
3. Select the print range and number of copies.
4. Click **OK**.
   The report is sent to the printer.

Export and save the report contents

You can export the report contents in a number of different file formats, including CSV, TSV, Excel, RTF, HTML, Microsoft Word, and plain text.

Note: Due to limitations of the Export utility, you may receive an error saying it cannot export the report contents.

To export and save a report

1. Generate a report.
2. On the Report Viewer toolbar, click **Export**.
3. In the Export dialog box, in the Format drop-down list, click the desired format.
4. In the Destination drop-down list, click the desired destination.

   For example, if you choose the file format "HTML 3.2 (Standard)" and the destination "Application," the Report Viewer will start the default browser with the report data loaded.
5. Click **OK**.
6. For some file formats, in the Number and Date Format dialog box, select the desired number and date formats and then click **OK**.
7. Do one of the following:
   - If you chose to export the data in an HTML format, in the Export to Directory dialog box, specify the desired directory and then click **OK**.
   - If you chose to export the data in a different format, in the Choose Export File dialog, specify the desired directory and file name and then click **OK**.

   Note: HTML exporting can produce multiple output files. In the Export To Directory dialog box, the directory name is not used to name an output file. It is used to create the directory where the HTML files will be created. By default, the base output file in this directory is named "default.htm." Point your browser at this file to view the report contents.

Enlarge the view area

The Zoom feature allows you to enlarge and shrink the size of the Report Viewer screen. With this feature, you can shrink the report to 25 percent or enlarge it to 400 percent of its original size.

To zoom in or out of a report

1. Generate a report.

2 On the Report Viewer toolbar, in the resize drop-down list, click the desired size.
The report changes to the selected size.

Locate information in a report

To locate information in a report

1. Generate a report.
2. On the Report Viewer toolbar, in the Search text box, type the desired text and then click **Search**.
3. To locate the next instance, click **Search** again.

Exit the report

To exit the report

◆ In the Report Viewer window, click the **X** in the upper right-hand corner.

Generating Agent status reports

Intruder Alert offers three reports that provide valuable information about an Agent system. Agent reports include:

- Agent Policy report
- Agent Active Datastream report
- Agent Load report

These reports are generated from and viewed in Intruder Alert Event Viewer. This requires that the Intruder Alert Reports policy is activated on the Agent system. The Intruder Alert Reports policy is automatically installed and activated on the Agent during installation. However, it may have been deactivated by an administrator. Prior to generating the Agent reports, verify that the Intruder Alert Reports policy is activated on the Agent.

The following sections describe each Agent report.

Agent Policy report

The Agent Policy report contains information about each activated policy since the Agent started or the policy was last modified. Report contents include:

- Agent name

- When the Agent started
- Policies activated on the Agent
- Date and time the policy was last modified
- Number of times each rule was executed

Agent Active Datastream report

The Agent Active Datastream report lists the status of each event source. Intruder Alert has different event sources for each supported operating system. The event sources on UNIX include, syslog, wtmp, process accounting and, where available, btmp and C2 audit logs. Event sources for Windows systems include System, Application, and Security logs.

The Agent Active Datastream report lists active event sources on the selected Agent. If the Agent reports were generated on a UNIX Agent, the report will list each datastream (event source) and whether the datastream is active or inactive.

Note: If a data stream is inactive, perform necessary troubleshooting to determine why and reestablish it as a source of events.

Agent Load report

The Agent Load report lists statistics describing the activity or load on the Agent. These statistics include the number of times a Manager has connected to the Agent and the total events processed. Total events processed encompass Intruder Alert Status events, Intruder Alert Error events, and System Message events from each event source, including those from user-defined audit logs.

Generate an Agent report

The Agent reports are generated by sending the Agent an Intruder Alert command called “report.” The report command generates three events on the Agent system that correspond to the three Agent reports described above.

To view the report data, generate a new text view in Intruder Alert Event Viewer with only the Intruder Alert Reports policy and the Agent system selected.

To generate and view the Agent reports

1 Verify that the Intruder Alert Reports policy is active on the Agent system.
The Reports policy is automatically activated on each Agent during installation, but if it has been removed, you must reapply it.
See “Applying policies to a domain” on page 127.

2 On the Event Viewer menu bar, click **ITA > Send Intruder Alert Command**.
See "Sending an Intruder Alert command to an Agent" on page 191.

3 In the **Send ITA Command** dialog box, in the Commands text box, type:
`report`

4 Make selections for the Manager and Agent fields in the dialog box and then click **Send Command**.

5 On the Event Viewer menu bar, click **File > New Query**.
See "Creating a new view" on page 185.

6 In Query Builder wizard screen one, in the View Type drop-down list, click **Text**. Fill in the other fields in screen one and then click **Next**.

7 In Query Builder wizard screen two, click **Next**.

8 In Query Builder wizard screen three, in the Manager Objects box, click **ITA Reports** and then click the right-arrow to move it to the Query List box.

9 In the Manager Objects box, click the Agent system object and then click the right-arrow to move it to the Query List box.

10 Click **GO!**.
The Text View screen appears with the Agent report events listed. The Agent report events are the three Agent reports as described above.

11 Click on the first event to view the Agent Load report, the second event to view the Agent Policy report, and the third event to view the Agent Active Datastream report.
The contents of the report are viewable in the lower half of the Text View screen.

Section 5

Appendices

This section discusses the following:

- Appendix A: Contacting customer support
- Appendix B: Operating system collectors
- Appendix C: ita.ini file documentation
- Appendix D: Optimization and problem solving techniques
- Appendix E: SNMP for Intruder Alert
- Appendix F: Destination ports for Intruder Alert

Contacting customer support

Customer support

Symantec's technical support group of skilled technical engineers provide platform-specific information about Symantec products. Our staff has in-depth expertise in both client/server computing and information security technology.

Before contacting technical support

See the on-line help, the relevant portion of the administration guide, or the release notes for the version of the Symantec product. If you are not able to find a solution, access Symantec's Web site at:

http://www.symantec.com/techsupp/

If you are unable to find a solution, complete the following steps before calling Technical Support:

- Become an authorized contact with your security manager.
- Check on the Web for tune-up packs or updates for your product and review the technical FAQ's.
- Be at the computer, so our technical engineers can talk you through the steps needed to correct the problem.
- Gather the relevant information described in the tables on the following pages.

Table A-1 Required Administrator or Event Viewer information

Information	Source
Machine Type:	Get from Windows "System Properties" dialog.

Table A-1 Required Administrator or Event Viewer information

Information	Source
OS Level:	Get from Windows "System Properties" dialog.
Version:	Get from the Help menu's About Intruder Alert dialog.
Date:	Get from the Help menu's About Intruder Alert dialog.

Table A-2 Required Manager information

Information	Source
Machine Type:	Get from "uname -a" if UNIX or "System Properties" if Windows.
OS Level:	Get from "uname -a" if UNIX or, "System Properties" if Windows.
Version & Date:	Get from the file /axent /ita/bin/Revision.txt if UNIX or Program Files\Symantec\ITA\bin\Revision.txt if Windows. Also check the Manager Properties dialog in the security product console.

Table A-3 Required Agent information

Information	Source
Machine Type:	Get from "uname -a" if UNIX or "System Properties" if Windows.
OS Level:	Get from "uname -a" if UNIX or "System Properties" if Windows.
Version & Date:	Get from the file /axent /ita/bin/Revision.txt if UNIX or Program Files\Symantec\ITA\bin\Revision.txt if Windows. Also check the Agent Properties Item in the Agent Context Menu in the security product console
International version:	Check the Agent.log file for the message "Initializing international level encryption."

Table A-4 Required network information

Information
Find out the network protocol used (Vendor/version).

Table A-5 Required problem information

Information
List all the steps needed to reproduce the problem.
Describe the symptoms of the problem.
Note the exact wording of any error messages (every character counts).
Print, fax, or email copies of the system log files.
Provide any other relevant information about the problem.

Finding version and platform information on the Web

For a complete list of recent Intruder Alert build versions and associated platforms, use the following procedure.

To find version and platform information on the Web

1. Go to the Symantec Web site:
   http://www.symantec.com/techsupp/enterprise/
2. Under the heading Technical Support, click **knowledge base**.
3. On the next Web page, under the heading Intrusion Protection, expand **Symantec Intruder Alert**.
4. Click the version that matches yours.
   If you click **Inactive versions**, then on the next Web page you must click **Knowledge Base** under the specific version.
5. On the next Web page, on the Search tab, in the text box, type:
   `latest build`
6. Click **search**.
7. On the next Web page, click the link to the article whose title and description match the desired information.
   The latest build and platform information should be in the first article.

Contacting technical support

To contact Symantec's technical support, see the Technical Support section at the beginning of this guide.

Appendix B

Operating system collectors

This appendix contains information on the following topics:

About collectors

A collector collects data to be analyzed by Intruder Alert. This appendix describes the collectors for each of the supported operating systems: UNIX and Windows. Where applicable, it contains instructions for configuring Intruder Alert to monitor additional sources.

UNIX collectors

Intruder Alert automatically monitors the following UNIX audit logs, unless otherwise noted:

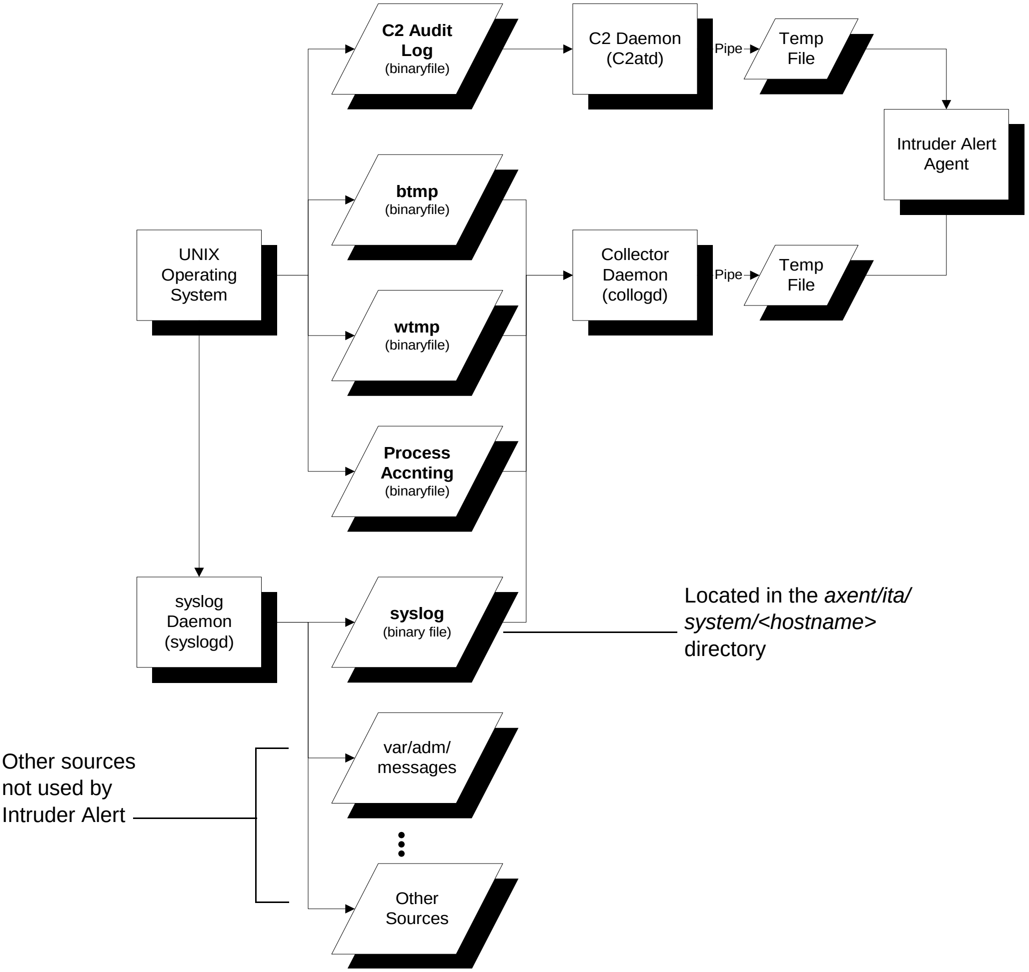
- syslog
  syslog contains operating system messages.
- wtmp, wtmps
  wtmp and wtmps collect login and accounting information.
- btmp, btmps
  btmp and btmps collect failed login information. btmp is not available on all UNIX platforms.
- Process accounting
  Process Accounting collects user process information and numerous other processing activities.

A syslog file is located in the axent/ita/system/<hostname> directory, and receives event data from the syslog daemon.

A collector daemon, collogd, reads the collector files and pipes event data to the Agent. The Agent then processes the event according to its activated policies.

The following diagram illustrates how Intruder Alert captures and processes events on UNIX systems.

Figure B-1 Event collection on UNIX



The audit source files (as an example, syslog, wtmp, and so forth) will continue to grow until those files are truncated.

The size of these files can be managed manually or Intruder Alert's collogd daemon can be configured to manage their growth automatically (via settings in the ita.ini file).

See "Manage the size of UNIX collectors" on page 265.

Note: The ability to audit these sources depends on the type of platform and installed platform options.

Configure Intruder Alert to monitor C2 collector

The United States Department of Defense (DOD) established a set of standards for different levels of information security. These standards are published in the *Trusted Computer System Evaluation Criteria* document, also known as the "Orange Book." The DOD organized these standards in four groups called A, B, C, and D, with seven levels. From highest to lowest, these levels are: A1, B3, B2, B1, C2, C1, and D.

At the C2 level, data must be protected so that it is available to only single users. In addition, C2 requires that an audit trail track access and attempted access to objects in the environment. Many operating system vendors now offer C2 auditing to their customers as a configurable option.

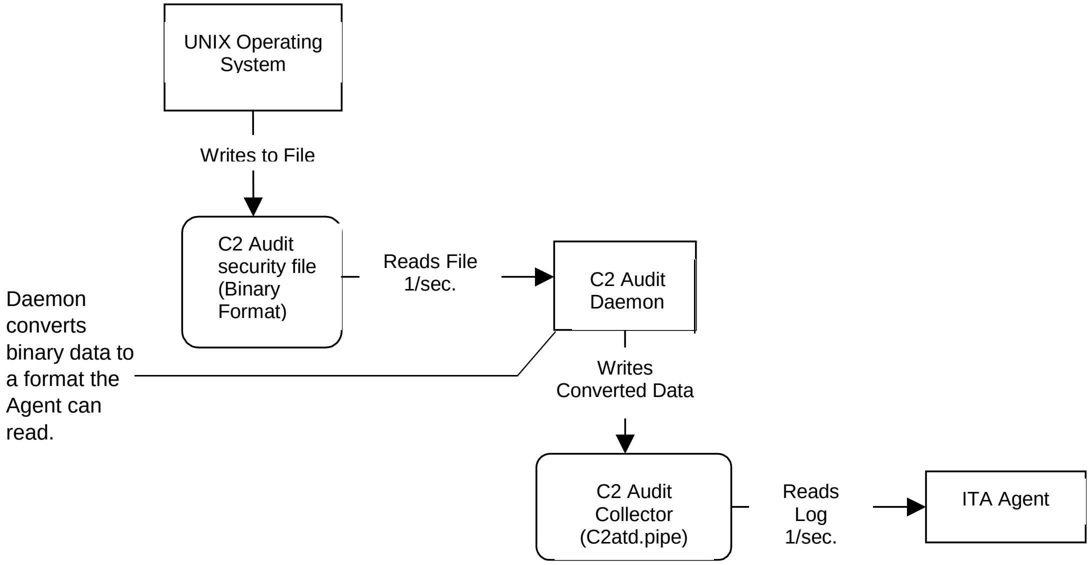
After C2 has been configured in the operating system, Intruder Alert can be configured to monitor the C2 audit log created by the operating system. Intruder Alert can monitor C2 audit pipes on HP-UX, Solaris, and OSF/1.

The process for configuring C2 auditing consists of three main steps or phases. They include:

- Configuring the UNIX system to utilize C2 audit logging. (For instructions, refer to the UNIX documentation that shipped with the operating system.)
- Initializing and configuring the C2 auditing daemon in the ita.ini file.
- Configuring the Agent to watch the C2atd.pipe.

The UNIX operating system writes C2 data to a binary C2 auditor. The C2 audit trail daemon translates the binary data into a format the Agent can read. The Agent then reads the information and processes it. The following graphic illustrates this process.

Figure B-2 C2 audit processing


UNIX Operating System
Writes to File
C2 Audit security file (Binary Format)
Reads File 1/sec.
C2 Audit Daemon
Daemon converts binary data to a format the Agent can read.
Writes Converted Data
C2 Audit Collector (C2atd.pipe)
Reads Log 1/sec.
ITA Agent

Configure the C2 audit daemon

Two settings added to the ita.ini file initialize and configure Symantec's C2 audit trail daemon. The first command is required and starts the daemon.

The second command is optional. It allows the user to specify options when using the daemon, including the frequency, in seconds, to read the C2 binary audit pipe.

There are three different options available when configuring C2:

- -p 'x': wait 'x' seconds between polls.
- -i 'y': use alternate 'y' audit file interpreter.
- -b: reads from beginning of audit file.

To initialize and configure the C2 audit daemon

1 Open the ita.ini file into a UNIX text editor.
The ita.ini file is located in the axent/ita/system/<hostname> directory, where <hostname> represents the name of the system being configured.

2 At the end of the [Agent] section, create a new line and enter the following command:

```
C2ATD_START=1
```

The setting 1 starts or enables the daemon, and the setting 0 disables or prevents the daemon from starting.

3 Optionally add another line and enter the following command:

```
C2ATD_OPTIONS= -px
```

where x represents how often (in seconds) the daemon reads the C2 audit pipe. The default is every second. In the following example, the daemon would read the pipe every 3 seconds.

```
C2ATD_OPTIONS= -p3
```

4 Save the changes to the ita.ini file.

5 Stop and restart the Agent.

See "Starting and stopping Managers/Agents" on page 66.

This phase of configuring Intruder Alert to monitor a C2 audit pipe is complete. The Agent must be configured to monitor the output file created by the daemon.

Configure Intruder Alert to monitor the C2 audit pipe

To configure Intruder Alert to monitor the C2 audit pipe

1 Start Intruder Alert Administrator and connect to a Manager.

2 Expand the Manager's branch.

3 In the Registered Agents branch, click the desired Agent.

4 In the right pane, in the Agent configuration fields, right-click in the Audit Logs box and then click **New** in the drop-down list.

5 In the Audit Pipe dialog box, type a description in the Description field and then press **Tab**.

6 In the File Name text box, type:

/axent/ita/system/<hostname>/C2atd.pipe

where <hostname> represents the name of the system being configured.

For example:

```
/axent/ita/system/juggler/C2atd.pipe
```

7 Click **Multiple Line**, and specify a record delimiter for the type of operating system being configured. Refer to the following table.

Table B-1 C2 audit pipe record delimiters

On	Enter
HP-UX	~~~~~~ (Five or six tildes is sufficient to identify a new record.)
Solaris	return (The word “return” serves as the record delimiter.)
Digital UNIX OSF/1	\n (Identifies a blank line.)

8 On Solaris systems, check **Include Delim**.
The line containing the delimiter is part of the message.

9 Optionally click in the text box, and type the event string or strings to parse.
Parsing allows you to gather specific information from an event message and use that information for reporting in the Intruder Alert Event Viewer. Use the following guidelines for parsing events.

Table B-2 Parsing guidelines

To	Use
Label Parsed Fields (Intruder Alert captures whatever information appears in braces ({})and stores it for Intruder Alert Event Viewer reporting. The user-defined label identifies the data.)	{Name of Field} Braces {}, not square brackets [].
Represent spaces	Press the spacebar
Represent carriage returns/line endings	\n
Represent single missing characters	?
Represent multiple missing characters or words	*

The following is an example event message:

```
event:chanc logged on to Juggler at 14:05 on 03/18/01
```

The following parsed string captures the relevant information contained in that event.

```
event:{User} {Action} to {System} at {Time} on {Date}
```

If no additional parsing rules are defined, Intruder Alert applies standard parsing rules to each message (for example: Date, Time, Value, Agent, Policy, Rule, User, and Message Text).

10 Click **OK**.

The Agent is now configured to monitor the selected C2 audit log.

Windows collectors

Intruder Alert uses the following event collectors to monitor Windows activities:

- Event log collector
- File watch collector
- Custom log file collector
- Windows Registry collector

Event log collector

Intruder Alert captures events through the system audit logs and the Windows Registry.

Intruder Alert can filter any audit, security or other type of log on a real time basis. Intruder Alert can monitor as many logs as necessary. However, care should be taken to target policies and their rules to capture only important events. Otherwise, performance will suffer and numerous nonvital events will be captured by Intruder Alert.

Numerous options are available to the Windows system administrator to monitor events of interest for the server. Intruder Alert provides stock policies for typical Windows audit functions. The Intruder Alert security administrator may add further auditing with Custom Log collectors.

In the Intruder Alert versions 3.6 and above, there are three new Windows Server event collection capabilities for advanced intrusion detection system administrators looking for further policy customization capabilities. The three event collectors, Directory Service, DNS Server, and File Replication enable the collection (via custom policy creation) of events that occur in the directory service, DNS server, and from server to server, respectively.

Windows has three basic system audit log sources:

- Security
- Application
- System

About auditing

The Windows audit policy in Event Viewer defines the security related events to monitor and log in the Windows Security event log. The Security event log is viewable from the Windows Event Viewer.

Intruder Alert turns on Windows event logging, but not all security-related events are required for Intruder Alert to successfully operate.

The following are the default audit events for Windows.

Table B-3 Windows recommended audit policy

Action	Success	Failure
Audit account logon events	X	X
Audit account management	X	X
Audit directory service access		X
Audit logon events	X	X
Audit object access	X	X
Audit policy change	X	X
Audit privilege use		X
Audit process tracking		X
Audit system events	X	X
Audit account logon events	X	X

Additional functionality in the event log collector

In Intruder Alert version 3.6.1, the event log collector is enhanced to provide finer granularity in the processing of event log records. This is done with two additions in functionality:

- First, the Event Record selection criteria is expanded to allow optional selection based upon Event ID and Event DOMAIN/USER.
- Second, you can now exclude events.

To support these new features, there are some changes to the syntax of the file cols_nt.cfg. The cols_nt.cfg file contains a complete list of the event sources that Intruder Alert automatically monitors. You can configure Intruder Alert to capture events from additional event sources by adding entries to cols_nt.cfg.

See "Default Registry auditing" on page 233.

The new syntax is as follows:

```
 [-]\<log name>\<event source>[[\<event id>][\<event domain/user>]]
```

where:

- <event id> is the numerical category ID that is associated with each event record. The wild card characters '*' and '?' can be used in the criteria.
- <event domain/user> is the user name qualified with the domain name. It is important that the domain name be specified first and the forward slash character ('/') be used to separate the domain and user name. The wild card characters '*' and '?' can be used in this criteria.

To specify that a selection criteria entry be used to exclude event records, prepend the line with a minus sign ('-').

For example, to filter out all of the successful logout events for the domain 'MYDOMAIN', use the following:

```
-\security\security\538\MYDOMAIN/*
```

To filter out all of the successful logon events for the user 'john_doe' in the domain 'MYDOMAIN', use:

```
-\security\security\528\MYDOMAIN/john_doe
```

In addition the above changes to the collector, entries have been made to cols_nt.cfg to filter out the 'Object Access' auditing events. If this is undesired, simply comment out the last few event exclusion lines in cols_nt.cfg.

File watch collector

The file watch collector is covered elsewhere.

See "File and directory security" on page 147.

Custom log file collector

This feature of Intruder Alert lets you monitor any text file on the system, whether it is created by you or some application program. Once you have configured Intruder Alert, it will read the file as one of its own audit logs and report events based on the information in the file.

The custom log file collector gives you two file watch options. They are single line and multiple line. The single line collector works with a carriage return while the multiple line collector requires that you enter some type of delimiter.

Whether single line or multiple, the custom log file collector must be configured from an active agent and will only work on the agent.

To create a single line collector

1. In Intruder Alert Administrator, connect to an Agent.
2. In the right pane, under Audit Logs, click **New**.
3. In the Audit Log window, click **Single Line**.
4. In the Description text box, type a description of the file you will monitor.
5. In the File Name text box, type a fully qualified path to the file you wish to monitor.
6. In the Strings to Parse text box, type the desired pattern to audit.
7. Click **OK**.
8. In the Audit Logs box, click the name of the new audit log and then click **Save**.
   The audit log collector is not complete until you save it.
   The audit log is configured, but will not generate events until you create a rule that will trigger events based on the contents of the log.
   See "Adding and deleting a rule" on page 139.

To create a multiple line collector

1. In Intruder Alert Administrator, connect to an Agent.
2. In the right pane, under Audit Logs, click **New**.
3. In the Audit Log window, click **Multiple Line**.
4. In the Description text box, type a description of the file you will monitor.
5. In the File Name text box, type a fully qualified path to the file you wish to monitor.
6. In the Delim String text box, type your delimiter string.
   The text entered as the delimiter string replaces the carriage return as the EOL marker. If you check **Include Delim**, the text delimiter is included in the information passed to the Intruder Alert Event Viewer.
7. In the Strings to Parse text box, type the desired pattern to audit.
8. Click **OK**.

9 In the Audit Logs box, click the name of the new audit log and then click **Save**.

The audit log is not complete until you save it.

The audit log is configured, but will not generate events until you create a rule that will trigger events based on the contents of the log.

See "Adding and deleting a rule" on page 139.

To delete a custom log file collector

1 In Intruder Alert Administrator, connect to an Agent.

2 In the right pane, under Audit Logs, click the audit log you want to delete.

3 Click **Delete**.

4 Click **Save**.

Note: If you do not click Save, the agent will continue to monitor the deleted audit log, but it will not show up in the list of Audit Logs.

Windows Registry collector

Windows stores all configuration information in a database called the Registry. The Registry is a hierarchical database that controls all of the information related to the Windows operating system. The Windows system configuration, hardware configuration, configuration information about Win32-based applications, user preferences, and group policies are all stored in the Registry. For example, any Windows computer access changes or user changes on the computer are immediately reflected in the Registry. Because of these characteristics, the Registry serves as the foundation for user, system, and network management in Windows.

How Intruder Alert uses the Registry

Though Registry auditing has always been available through the Windows program, regedt32, there are many "audits" that generate false positives. This is because when a program opens a key for access, the program has to inform the Registry what kind of access to the key is needed. Software developers typically select "full" access to keep things simple. The auditing feature in the Registry is tied to how the key was opened, not necessarily how it was accessed, resulting in false positives.

The Intruder Alert Registry monitoring capabilities are based on a device driver that monitors access to the Windows registry by registry key. Intruder Alert, with its Registry Auditing capabilities and its Registry Key command, lets you safely monitor the Registry. False positives are reduced to a minimum because only the key or value needed and Intruder Alert audits how it is accessed.

Implementing Registry auditing in an Intruder Alert policy lets you create a rule that uses the Select Windows Registry Key criteria. In the rule, you can add the desired Action so that Intruder Alert can respond to any suspicious Windows Registry activity. All events are sent to the Event Viewer by default. Other than configuring the policy and rule, the Registry monitoring capabilities require no additional configuration by the user.

Using these features of Intruder Alert makes Registry monitoring much easier. Otherwise, the user would have to figure out how to find the Registry keys, then turn on the auditing, and then create a rule in Intruder Alert.

The load of the auditing is virtually undetectable. The Intruder Alert registry auditing takes very few CPU cycles and no disk access. This keeps the auditing load to the absolute minimum.

Intruder Alert 3.6 enhancements

We can look at the Windows Audit Tampering policy in Intruder Alert 3.6 as an example of added capability and protection available through use of the Registry monitoring.

The Windows Audit Tampering policy checks for seven events:

- Changing the audit policy
- Clearing the event log
- Turning auditing off
- Turning auditing on
- System, Security, and Application log file size changes
- System, Security, and Application log file location changes
- System, Security, and Application event message expiration changes.

The last three checks would not be possible without Registry monitoring.

Default Registry auditing

The sources for the default Registry auditing are located in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog. The event source Registry keys are all below this starting point. On a typical Windows system, you could easily have over 400 possible audit sources under your starting point.

However, not all the possible event sources are monitored by Intruder Alert.

You can configure Intruder Alert to capture events from additional event sources by adding entries to the cols_nt.cfg file. Viewing this file also gives you a complete list of the event sources that Intruder Alert automatically monitors. The default event sources will vary depending on which version of Windows you are using.

The following is a partial list of the standard audit sources Intruder Alert automatically monitors.

- \system\Application Popup
- \system\system
- \system\RemoteAccess
- \system\BROWSER
- \system\Service Control Manager
- \system\Rdr
- \system\EventLog
- \system\NETLOGON

The first column in the list represents the logging service that handles the reporting application, and the second column specifies the application name as it appears in the Source column of the Event Viewer.

Intruder Alert can monitor additional sources specific to your environment, such as third-party applications that register themselves as event sources. In an application log, the application source is listed in the Source column. Intruder Alert can be configured to monitor any of these sources by adding the source to the cols_nt.cfg file.

To configure Intruder Alert to monitor additional sources

1. Open cols_nt.cfg using any text editor (for example, NotePad, WordPerfect, and so forth).
   The file is located in the following directory
   <system drive>:\Program Files\Symantec\ITA\system\<hostname>
2. Scroll to the bottom of the file, and insert the path to the audit source registry.
   For example:
   \application\Java VM
3. Save the file.
4. Stop and restart the Agent for the changes to go into effect.
   See "Starting and stopping a Windows Manager/Agent" on page 66.

The Registry key command

In addition to the file and Registry auditing capabilities that Intruder Alert provides, you now have the ability to write custom rules to monitor any Registry key. This feature is new with Intruder Alert 3.6 and provides you with extensive customization capabilities.

- You decide which Registry keys and values to monitor and provide an alert.
- You monitor the actions of new Registry keys.
- You monitor attempts to effect the results of actions of Registry keys.
- You provide near real-time alerts.

The Registry Key Command gives you the capability to monitor the following:

- Close Key
  This function monitors the release of the Registry key you specify. Closing a Registry key does not necessarily write information to the Registry before ending; it can take as much as several seconds for the cache to be flushed to the hard disk. If an application or service must explicitly write registry information to the hard disk, it may use the flush function. If the Close Key function does not return the information you are looking for, you may want to try the Flush Key function.
- Create Key
  This function monitors the creation of subkeys or values within the Registry key you specify. Unless you specify a particular type of service or application, this function could register too many alerts to be of practical value
- Delete Key
  This function monitors the deletion of the Registry key you specify. The entire key, including all of its values, is removed.
- Delete Value
  This function monitors the deletion of a named value from the Registry key you specify.
- Enumerate Key
  This function monitors the enumeration of subkeys of the Registry key you specify. The specified key must have been opened first.
- Enumerate Value
  This function monitors the enumeration of the values for the Registry key you specify. The enumeration retrieves information about one subkey each time it is called. If the Registry key you specify has several subkeys, each alert on the Enumerate Value function will be displaying a different piece of information to the user.

- Flush Key
  This function monitors the writing of the attributes of the Registry key you specify into the registry. Flushing is an explicit command and writes all the attributes of the Registry key you have specified to the Registry immediately.
- Open Key
  This function monitors the opening of the Registry key you specify. Opening a specific key would be preparatory to performing some other action on the key, a subkey, or a value within the key.
- Query Key
  This function monitors the retrieval of information about the Registry key you specify. Before the key can be queried it must be opened, so you can monitor the opening with the Open Key function as well.
- Query Value
  This function monitors the retrieval of information about a specified value name associated with the Registry key you specify. Before the value can be queried its associated key must be opened, so you can monitor the opening with the Open Key function as well.
- Set Value
  This function lets you specify a particular service or application to which the rule you are creating will apply. For example, many applications create temporary share services. For example, if you are monitoring the Shares key, you will receive many alerts that you do not necessarily want.

Intruder Alert uses the Registry through a runtime loading collector. The collector operates through the agent. When the agent is stopped the collector unloads.

Creating a custom policy

There are two parts to auditing a Registry key. The first part generates a Registry filter rule that gets passed to the collector. This means the collector monitors only the keys needed. This reduces CPU overhead on the system and Intruder Alert.

The second half requires creating a standard rule that watches for the access to the Registry key.

Use the following scenario to create a custom policy in which you will store your custom rules.

You have a system configured for certain critical operations and want to know if any user attempts to change the PATH settings.

The procedures in this section explain how:

- To create a custom policy
- To create a custom filter rule within your policy
- To define information passed to the collector
- To create a second custom rule for actions

You must also define the action to be taken when the rule is activated.

See "Actions" on page 106.

The scenario for creating your custom policy is that you are monitoring the computer and want to design a custom rule that will alert you if anyone tries to change the PATH settings.

To create a custom policy

1. Launch Symantec Intruder Alert Administrator.
2. Connect to a Manager.
3. In the left pane, click the plus sign (+) to the left of the Manager to expand the view.
4. Right-click **Policies** and then click **New** in the drop-down list.
5. In the right pane, in the Label text box, type:

   `Test`
6. Press **Tab**.
7. In the Description text box, type:

   `Test Policy`

   You have created a policy on your system. It has no rules and it has not been applied to any domains or computers.

To create a custom filter rule within your policy

1. In the left pane, click the plus sign (+) to the left of your new policy to expand the view.
2. Right-click **Rules** and then click **New** in the drop-down list.
3. In the right pane, in the Label text box, type:

   `Path - Filter`
4. Press **Tab**.
5. In the Description text box, type:

   `This rule will inform you if anyone attempts to change, or changes, the PATH settings.`

6 In the Rule Value text box, type:

0

7 Click **Indirect**.

8 In the left pane, click the plus sign (+) to the left of your new rule to expand the view.

9 Right-click **Select** and then click **New > Windows Registry Key** in the drop-down list.

10 In the Process Name text box, type:

*****

This will let you monitor all processes accessing the registry value.

11 In the Key Name field, type:

```
\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Session
Manager\Environment\Path
```

The asterisk on either side of the ControlSet word allows the filter to monitor the CurrentControlSet, ControlSet001, and ControlSet002 at the same time.

You have selected the Registry keys you are going to monitor.

To define information passed to the collector

Now define the information your filter will pass to the collector.

The information on this computer is very important and you want to know immediately if someone has attempted to modify the PATH settings.

1 In the Actions area, click **Delete Value**.

2 Check **Success**.

3 Check **Failure**.

4 In the Actions area, click **Set Value**.

5 Check **Success**.

6 Check **Failure**.

You have created the filter that the collector needs to monitor the registry. Your filter will monitor any attempted change, or attempted change, to the PATH settings.

When monitoring a Registry key, as opposed to a Registry value, use the Create Key and Delete Key options. These four options will cover most of what you will monitor.

You have created a policy, a filter, and defined the information to be passed to the collector. Now create the second rule and select the actions to be performed when your rule causes a response in Intruder Alert.

To create a second custom rule for actions

1. In the left pane, click the plus sign (+) to the left of your new policy to expand the view.
2. Right-click **Rules** and then click **New** in the drop-down list.
3. In the right pane, in the Label text box, type:
   ```
   System Path Changed
   ```
4. Press **Tab**.
5. In the Description text box, type:
   ```
   This rule will inform you if anyone attempts to change, or
   changes, the PATH settings.
   ```
6. In the Rule Value field, type:
   ```
   50
   ```
7. In the left pane, click the plus sign (+) to the left of your new rule to expand the view.
8. Right-click **Select** and then click **New > System Message** in the drop-down list.
9. In the New Entry text box, type:
   ```
   *\HKEY_LOCAL_MACHINE\SYSTEM\*ControlSet*\Control\Session
   Manager\Environment\Path*
   ```
10. Right-click **Actions** and then click **New > Record to Event Viewer** in the drop-down list.

    You could select any of the fourteen valid choices for the action your rule will perform. Each choice has different properties.

    See "Actions" on page 106.
11. Click **Add to List**

    You have selected the Registry keys you are going to monitor. This policy will notify you whenever a user changes the system PATH variable, or attempts to change it.

Appendix C

ita.ini file documentation

This appendix contains the current default settings for files specified in the program ini files.

Windows

```
#############################################
[Agent]
#############################################
# Filewatch configuration files.  These contain the list of files
# that filewatch is monitoring.
filewatch=#ita\system\#system\ntcrit_L.lst,ntcrit_L
filewatch=#ita\system\#system\ntcrit_S.lst,ntcrit_S

# Turns on address caching. ON or OFF.
ADDR_CACHE = OFF

# Specifies how long the agent will use a cached address before
# trying to look up again (in minutes). The minimum is 15 minutes,
# the maximum is 48 hours.
ADDR_CACHE_TIMEOUT = 60

# Communications timeout (in seconds). The default is 30 seconds.
ITA_TIMEOUT = 30

# How long before the agent negotiates a new encryption key (in
# seconds). The default is 24 hours.
ENCRYPTION_KEY_LIFETIME = 86400
```

```
# How often the agent checks for expired keys (in seconds). The
# default is 60 minutes.
ENCRYPTION_KEY_CHECK_INTERVAL = 600

# Configure agent command restrictions. This file contains all
# commands that the ITA agent is allowed to execute via an
# "Execute Command" Action.
# NOTE: If no file is specified or the file does not exist, then no
# commands will be allowed.
ITA_COMMAND_LIST = #ita/system/#system/commands.txt

# Specifies how large (in bytes) the agent cache files are allowed
# to be. Default and maximum are 10000000.
MAX_CACHE_SIZE = 10000000

# How often the agent checks for changes to the cols_nt.cfg file (in
# seconds) The default is 60 seconds
NT_EVENT_TIMER = 60

# How many events to process before checking for other work.
# The default is 20.
# For each event source, this number is multiplied by the following:
# NT Event Log and Registry: 1
# Single-line external file: 2
#  Multi-line external file: 2
MAX_EVENTS_PER = 20

# Specified if agent will advertise (SAP) via IPX/SPX. ON or OFF.
SAP_ENABLE = OFF

# Specifies the maximum amount of time reading a single-line or
# multi-line external file (in seconds). The default is 2, the
# minimum is 1, and the maximum is 10.
LOG_MAX_SECONDS_PER = 2

############################################
```

```
[Manager]
############################################
# Turns on address caching. ON or OFF.
ADDR_CACHE = OFF

# Specifies how long the manager will use a cached address before
# trying to look up again (in minutes). The minimum is 15 minutes,
# the maximum is 48 hours.
ADDR_CACHE_TIMEOUT = 60

# Specifies a group of ports that will be used for communication
# with agents using the format: [<PORT NUM> | <PORT_RANGE_BEGIN> -
# <PORT_RANGE_END> ][, [<PORT NUM> | <PORT_RANGE_BEGIN> -
# <PORT_RANGE_END> ]] ...
# Maximum value for a port number is 65535.
# For example: TCP_PORTS = 10,20-30
# TCP_PORTS =
# Specifies a group of sockets that will be used for communication
# with agents
# SPX_SOCKETS =

# Communications timeout (in seconds). Default is 15 seconds.
ITA_TIMEOUT = 15

# Maximum number of delayed connects. Default is 20. Minimum is 500.
#MAX_DELAYED_CONNECTS = 20

# Maximum number of pending delayed connects. Default is 10000.
# Minimum is 5.
MAX_PENDING_CONNECTS = 10000

# Specifies the maximum number of records per batch to send to a
# query. The default is 500.
FILTER_BLOCK_SIZE = 500

# Specifies how large the .rex file will get before it rolls to a
# .ext file (in bytes). The default is 2MB.
```

```
RCACHE_EXTENT_SIZE = 2000000

# Specifies how large (in bytes) the manager cache files are allowed
# to be. Default and maximum are 10000000.
MAX_CACHE_SIZE = 10000000

# Allow old agents to connect to this manager
OLD_AGENTS_ALLOWED = 1

# Specified if manager will advertise (SAP) via IPX/SPX.
SAP_ENABLE = OFF

############################################
[Agent Diagnostics]
############################################
# Specifies if log file to be kept open while the Agent is running
# (0 = False, 1 = True)
LogFileKeepOpen = 1
# Enables or disables diagnostic reporting
Enable = 0
# Specifies how large the agent.log file will get (in KB)
MaxLogSize = 50
# Specifies how many old log files the agent will keep
MaxLogFiles = 2
# Includes the time with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogTimeStamp = 1
# Includes the date with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogDateStamp = 1
# Includes the name of the diagnostic group with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogGroupName = 0
# Includes the name of the diagnostic level with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogLevel = 0
# Will log diagnostic messages to standard out (if not run as a
# daemon) (0 = OFF, 1 = ON)
LogStdout = 0

# Diagnostic group names and levels.  The number specifies the
# lowest level for which you want to see diagnostic information.
# Thus, setting it to level 3 will also include levels 1 and 2.

# Main program loop
MOD_MAIN = 1
# Communications
MOD_COMM = 1
# Authentication
MOD_AUTH = 1
# Encryption
MOD_ENCRYPT = 1
# Manager Event Database
MOD_DB = 1
# Manager event cache
MOD_CACHE = 1
# Configuration Database
MOD_ISAM = 1
# Collectors
MOD_COLLECT = 1
# Event processing
MOD_EVENT = 1
# Event actions
MOD_ACTION = 1
# Dot format
MOD_DOT = 1
# Callback engine
MOD_CALLBACK = 1
# Memory manager
MOD_MEM = 1
# Policy updates
MOD_POLICY = 1

############################################
```

```
[Manager Diagnostics]
############################################
# Specifies if log file to be kept open while the Manager is running
# (0 = False, 1 = True)
LogFileKeepOpen = 1
# Enables or disables diagnostic reporting
Enable = 0
# Specifies how large the manager.log file will get (in KB)
MaxLogSize = 50
# Specifies how many old log files the manager will keep
MaxLogFiles = 2
# Includes the time with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogTimeStamp = 1
# Includes the date with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogDateStamp = 1
# Includes the name of the diagnostic group with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogGroupName = 0
# Includes the name of the diagnostic level with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogLevel = 0
# Will log diagnostic messages to standard out (if not run as a
# daemon) (0 = OFF, 1 = ON)
LogStdout = 0

# Diagnostic group names and levels.  The number specifies the
# lowest level for which you want to see diagnostic information.
# Thus, setting it to level 3 will also include levels 1 and 2.

# Main program loop
MOD_MAIN = 1
# Communications
MOD_COMM = 1
# Authentication
MOD_AUTH = 1
```

```
# Encryption
MOD_ENCRYPT = 1
# Manager Event Database
MOD_DB = 1
# Manager event cache
MOD_CACHE = 1
# Configuration Database
MOD_ISAM = 1
# Collectors
MOD_COLLECT = 1
# Event processing
MOD_EVENT = 1
# Event actions
MOD_ACTION = 1
# Dot format
MOD_DOT = 1
# Callback engine
MOD_CALLBACK = 1
# Memory manager
MOD_MEM = 1
# Policy updates
MOD_POLICY = 1

############################################
[GUI]
############################################
# Specifies if TCP/IP or IPX/SPX (or both) will be used.
# 1 specifies TCP/IP only.
# 2 specifies IPX/SPX only.
# Any other value specifies both.
PROTOCOL = 0

# Communications timeout (in seconds). This setting will only affect
# the Mgr/Agt Setup program and the Administrator.
# The default is 60 seconds.
ITA_TIMEOUT = 30
```

```
# Specifies the port to listen on. This setting will affect the
# Administrator program. The default is 3833.
ADMIN_SERVER_PORT = 3833

# The maximum number of records to show in the event viewer.
# Default is 15000.
VIEWRECORDS = 15000

############################################
[ADMIN]
############################################
# Specifies the port to listen on. This setting will only affect the
# Mgr/Agt Setup program. The default is 2840
SERVER_PORT = 2840

############################################
[Admin Diagnostics]
############################################
# Specifies if log file to be kept open while the Admin is running
# (0 = False, 1 = True)
LogFileKeepOpen = 1
# Enables or disables diagnostic reporting
Enable = 0
# Specifies how large the admin.log file will get (in KB)
MaxLogSize = 50
# Specifies how many old log files admin will keep
MaxLogFiles = 2
# Includes the time with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogTimeStamp = 1
# Includes the date with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogDateStamp = 1
# Includes the name of the diagnostic group with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogGroupName = 0
# Includes the name of the diagnostic level with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogLevel = 0
# Will log diagnostic messages to standard out (if not run as a
# daemon) (0 = OFF, 1 = ON)
LogStdout = 0

# Diagnostic group names and levels.  The number specifies the
# lowest level for which you want to see diagnostic information.
# Thus, setting it to level 3 will also include levels 1 and 2.

# Main program loop
MOD_MAIN = 1
# Communications
MOD_COMM = 1
# Authentication
MOD_AUTH = 1
# Encryption
MOD_ENCRYPT = 1
# Manager Event Database
MOD_DB = 1
# Manager event cache
MOD_CACHE = 1
# Configuration Database
MOD_ISAM = 1
# Collectors
MOD_COLLECT = 1
# Event processing
MOD_EVENT = 1
# Event actions
MOD_ACTION = 1
# Dot format
MOD_DOT = 1
# Callback engine
MOD_CALLBACK = 1
# Memory manager
MOD_MEM = 1
# Policy updates
```

```
MOD_POLICY = 1

############################################
[View Diagnostics]
############################################
# Specifies if log file to be kept open while the Event Viewer is
# running (0 = False, 1 = True)
LogFileKeepOpen = 1
# Enables or disables diagnostic reporting
Enable = 0
# Specifies how large the view.log file will get (in KB)
MaxLogSize = 50
# Specifies how many old log files the viewer will keep
MaxLogFiles = 2
# Includes the time with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogTimeStamp = 1
# Includes the date with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogDateStamp = 1
# Includes the name of the diagnostic group with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogGroupName = 0
# Includes the name of the diagnostic level with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogLevel = 0
# Will log diagnostic messages to standard out (if not run as a
# daemon) (0 = OFF, 1 = ON)
LogStdout = 0

# Diagnostic group names and levels.  The number specifies the
# lowest level for which you want to see diagnostic information.
# Thus, setting it to level 3 will also include levels 1 and 2.

# Main program loop
MOD_MAIN = 1
# Communications
```

```
MOD_COMM = 1
# Authentication
MOD_AUTH = 1
# Encryption
MOD_ENCRYPT = 1
# Manager Event Database
MOD_DB = 1
# Manager event cache
MOD_CACHE = 1
# Configuration Database
MOD_ISAM = 1
# Collectors
MOD_COLLECT = 1
# Event processing
MOD_EVENT = 1
# Event actions
MOD_ACTION = 1
# Dot format
MOD_DOT = 1
# Callback engine
MOD_CALLBACK = 1
# Memory manager
MOD_MEM = 1
# Policy updates
MOD_POLICY = 1

############################################
[UPC]
############################################
# ITA Host Name Resolution behavior.
# ITA_NAME_RESOLUTION=DNSONLY will force traditional hostname
# resolution and will reference the hosts file (DEFAULT)
# ITA_NAME_RESOLUTION=USEWINS will allow WINS information via a
# Win32 name resolution method
# ITA_NAME_RESOLUTION=USEALL will first try traditional hostname
# resolution, and if it fails to resolve the name it
# will attempt to via a Win32 name resolution method
```

```
ITA_NAME_RESOLUTION=DNSONLY
# ITA IP Bind setting
# ITA_BIND_ADDRESS=192.168.0.49
```

UNIX

```
############################################
[Agent]
############################################
# Filewatch configuration files.  These contain the list of files
# that filewatch is monitoring.
filewatch=#ita/system/#system/uxcrit_L.lst,uxcrit_L
filewatch=#ita/system/#system/uxcrit_S.lst,uxcrit_S
filewatch=#ita/system/#system/grabcore.lst,grabcore

# Turns on address caching. ON or OFF.
ADDR_CACHE = OFF

# Specifies how long the agent will use a cached address before
# trying to look up again (in minutes). The minimum is 15 minutes,
# the maximum is 48 hours.
# ADDR_CACHE_TIMEOUT = 60

# Communications timeout (in seconds). The default is 30 seconds.
ITA_TIMEOUT = 30

# How long before the agent negotiates a new encryption key (in
# seconds). The default is 24 hours.
ENCRYPTION_KEY_LIFETIME = 86400

# How often the agent checks for expired keys (in seconds). The
# default is 60 minutes.
ENCRYPTION_KEY_CHECK_INTERVAL = 600

# Configure agent command restrictions. This file contains all
# commands that the ITA agent is allowed to execute via an
# "Execute Command" Action.
# NOTE: If no file is specified or the file does not exist, then no
# commands will be allowed.
ITA_COMMAND_LIST = #ita/system/#system/commands.txt

# Specifies how large (in bytes) the agent cache files are allowed
# to be. Default and maximum are 10000000.
MAX_CACHE_SIZE = 10000000

# Unix Collector Truncation - Turning these on will let ITA manage
# the size of the SYSTEM files.
# NOTE: ITA will always control the size of its own files.  The
# MAX_SIZE entries are in KB. The minimum size is 64KB, the maximum
# size is 8192KB, and the default is 256KB.
   # Process Accounting
# ACCT_TRUNC = 1
# ACCT_LOG_MAX_SIZE = 512
   # Syslog
# SLOG_TRUNC = 1
# SLOG_LOG_MAX_SIZE=1024
   # WTMP
# WTMP_TRUNC = 1
# WTMP_LOG_MAX_SIZE = 512
   # BTMP - (Where available)
# BTMP_TRUNC = 1
# BTMP_LOG_MAX_SIZE = 512

# How many events to process before checking for other work. The
# default is 20.
# For each event source, this number is multiplied by the following:
#        Process Accounting: 4
#                    Syslog: 2
#             WTMP and BTMP: 1
# Single-line external file: 2
#  Multi-line external file: 2
MAX_EVENTS_PER = 20

# Specifies the maximum amount of time reading a single-line or
# multi-line external file (in seconds). The default is 2, the
# minimum is 1, and the maximum is 10.
LOG_MAX_SECONDS_PER = 2

# Indicates if the C2 Audit Trail Daemon should start when the agent
# starts
C2ATD_START = 0

# Options to be passed to the C2 Audit Trail Daemon
# -p x -- wait x seconds between polls
# -i y -- use alternate audit file interpreter y
# -b   -- read from beginning of the audit file
C2ATD_OPTIONS =

# Allow ITA to collect events from the process accounting file.
# Set to 1 to enable the process accounting collector.
# Set to 0 to disable the process accounting collector.
PROCESS_ACCOUNTING_ENABLED = 0

# On HP-UX 11.23 there are some system processes that still write
# useful information into the older /var/adm/wtmp and /var/adm/btmp
# databases.
# ITA's Collogd daemon monitors both the old databases and the newer
# /var/adm/wtmps and /var/adm/btmps databases if the version of
# HP-UX is 11.23 or greater. Uncomment the following 2 lines to
# instruct ITA to not monitor the older versions of the databases.
# ENABLE_OLD_WTMP = 0
# ENABLE_OLD_BTMP = 0

############################################
[Manager]
############################################
# Turns on address caching. ON or OFF.
ADDR_CACHE = OFF

# Specifies how long the manager will use a cached address before
# trying to look up again (in minutes). The minimum is 15 minutes,
# the maximum is 48 hours.
ADDR_CACHE_TIMEOUT = 60

# Specifies a group of ports that will be used for communication
# with agents
# TCP_PORTS =
# Specifies a group of sockets that will be used for communication
# with agents
# SPX_SOCKETS =

# Communications timeout (in seconds). Default is 15 seconds.
ITA_TIMEOUT = 15

# Maximum number of delayed connects. Default is 20. Minimum is 500.
#MAX_DELAYED_CONNECTS = 20

# Maximum number of pending delayed connects. Default is 10000.
# Minimum is 5.
MAX_PENDING_CONNECTS = 10000

# Specifies the maximum number of records per batch to send to a
# query. The default is 500.
FILTER_BLOCK_SIZE = 500

# Specifies how large the .rex file will get before it rolls to a
# .ext file (in bytes). The default is 2MB.
RCACHE_EXTENT_SIZE = 2000000

# Specifies how large (in bytes) the manager cache files are allowed
# to be. Default and maximum are 10000000.
MAX_CACHE_SIZE = 10000000

# Allow old agents to connect to this manager
OLD_AGENTS_ALLOWED = 1

############################################
[Agent Diagnostics]
```

```
############################################
# Specifies if log file to be kept open while the Agent is running
# (0 = False, 1 = True)
LogFileKeepOpen = 1
# Enables or disables diagnostic reporting
Enable = 0
# Specifies how large the agent.log file will get (in KB)
MaxLogSize = 50
# Specifies how many old log files the agent will keep
MaxLogFiles = 2
# Includes the time with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogTimeStamp = 1
# Includes the date with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogDateStamp = 1
# Includes the name of the diagnostic group with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogGroupName = 0
# Includes the name of the diagnostic level with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogLevel = 0
# Will log diagnostic messages to standard out (if not run as a
# daemon) (0 = OFF, 1 = ON)
LogStdout = 0

# Diagnostic group names and levels.  The number specifies the
# lowest level for which you want to see diagnostic information.
# Thus, setting it to level 3 will also include levels 1 and 2.

# Main program loop
MOD_MAIN = 1
# Communications
MOD_COMM = 1
# Authentication
MOD_AUTH = 1
# Encryption
```

```
MOD_ENCRYPT = 1
# Manager Event Database
MOD_DB = 1
# Manager event cache
MOD_CACHE = 1
# Configuration Database
MOD_ISAM = 1
# Collectors
MOD_COLLECT = 1
# Event processing
MOD_EVENT = 1
# Event actions
MOD_ACTION = 1
# Dot format
MOD_DOT = 1
# Callback engine
MOD_CALLBACK = 1
# Memory manager
MOD_MEM = 1
# Policy updates
MOD_POLICY = 1

############################################
[Manager Diagnostics]
############################################
# Specifies if log file to be kept open while the Manager is running
# (0 = False, 1 = True)
LogFileKeepOpen = 1
# Enables or disables diagnostic reporting
Enable = 0
# Specifies how large the manager.log file will get (in KB)
MaxLogSize = 50
# Specifies how many old log files the manager will keep
MaxLogFiles = 2
# Includes the time with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogTimeStamp = 1
```

```
# Includes the date with each diagnostic message logged
# (0 = OFF, 1 = ON)
LogDateStamp = 1
# Includes the name of the diagnostic group with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogGroupName = 0
# Includes the name of the diagnostic level with each diagnostic
# message logged (0 = OFF, 1 = ON)
LogLevel = 0
# Will log diagnostic messages to standard out (if not run as a
# daemon) (0 = OFF, 1 = ON)
LogStdout = 0

# Diagnostic group names and levels.  The number specifies the
# lowest level for which you want to see diagnostic information.
# Thus, setting it to level 3 will also include levels 1 and 2.

# Main program loop
MOD_MAIN = 1
# Communications
MOD_COMM = 1
# Authentication
MOD_AUTH = 1
# Encryption
MOD_ENCRYPT = 1
# Manager Event Database
MOD_DB = 1
# Manager event cache
MOD_CACHE = 1
# Configuration Database
MOD_ISAM = 1
# Collectors
MOD_COLLECT = 1
# Event processing
MOD_EVENT = 1
# Event actions
MOD_ACTION = 1
```

```
# Dot format
MOD_DOT = 1
# Callback engine
MOD_CALLBACK = 1
# Memory manager
MOD_MEM = 1
# Policy updates
MOD_POLICY = 1

############################################
[GUI]
############################################
# Communications timeout (in seconds). This setting will only affect
# the Mgr/Agt Setup program and the Administrator.
# The default is 60 seconds.
ITA_TIMEOUT = 30

############################################
[ADMIN]
############################################
# Specifies the port to listen on. This setting will only affect the
# Mgr/Agt Setup program. The default is 2840
SERVER_PORT = 2840

############################################
[UPC]
############################################
# ITA IP Bind setting
# ITA_BIND_ADDRESS=192.168.0.49
```

Appendix D

Optimization and problem solving techniques

This appendix includes the following topics:

- Optimizing system performance
- Known issues and resolutions

Optimizing system performance

This section describes how to configure and optimize certain aspects of Intruder Alert's performance.

The included topics are:

- Understand and manage the event database
- Delete old data
- Manage the size of Intruder Alert error logs
- Debug logging
- Configure the Record to Event Viewer action throttle
- Configure the email (SMTP) action throttle

Understand and manage the event database

The Record to Event Viewer action directs the Agent to record event/attack data in an event database located on the Manager's system. The Intruder Alert Event Viewer queries the database to generate online and printed reports.

Over time, event data accumulates on the Manager's system, consuming valuable disk space. This section describes how to control the amount of disk space being used.

The event database is comprised of two types of files, Rex (.rex) and Extent (.ext) files. These files reside in the following directory for each system type:

Windows:	<system disk>\Program Files\SymantecITA\system\<hostname>\
UNIX:	/axent/ita/system/<hostname>/

The most recent event data is contained in the .rex files. Only one rex file exists at a time on the Manager system. The default size of rex files is 2 MB. Extent (.ext) files contain archived event data. The size of these files is 2 MB.

Both the .rex files and .ext files are named with a number using the format <number>.rex. When a <number>.rex file reaches the maximum size, Intruder Alert writes final data to it, renames it to <number>.ext and creates a new file in the format <number + 1>.rex to hold new events.

For example, when the Manager is installed, Intruder Alert creates a 1.rex file and populates it with events. New Intruder Alert events are initially stored in the 1.rex file. When 1.rex reaches the maximum size, Intruder Alert writes final data to 1.rex, renames the file to 1.ext, and then creates the 2.rex file to hold new events. When 2.rex becomes full, the Manager writes final data to 2.rex, renames it as 2.ext and creates 3.rex to hold new events.

To display events, Intruder Alert opens the .rex file, reads the events in that file, looks at the number in the file name, and reads backwards through the .ext files that have a smaller number. For instance, if the current .rex file is 18.rex, Intruder Alert reads the events from 18.rex, from 17.ext, from 16.ext, and so on, in that order.

Extent files increment, starting with 1.ext and continue to the maximum number of 99999999.ext. With up to 99,999,999 possible extent files, there is no limit to the amount of data Intruder Alert can handle. The oldest extent files have the lowest number. For example, 1.ext will contain the oldest data; 2.ext will contain the next most recent data, and so on.

To control the size of .ext files stored in the directory, adjust the following setting found in the ita.ini file:

```
RCACHE_EXTENT_SIZE=
```

As Intruder Alert's administrator, you must decide how much and how far back data should be kept. Unneeded extent files should be archived and deleted from the Manager's system.

Note: When archiving the old files, it is crucial that the most recent .ext and .rex files not be removed. If the file is removed, Intruder Alert will create a new (empty) file beginning again with number 1.rex then 1.ext. The result will be discontinuity of event reporting and conflicting file names.

Delete old data

To delete unwanted data

1. Optionally archive the desired extent files.
2. Delete the desired files.

Note: If you delete old data, you may limit your view in Intruder Alert Event Viewer. This will occur if you specify a date that references data in an .ext file that was deleted or removed.

Corrupted .rex files

If Intruder Alert cannot read the .rex file, all event data is lost. The Intruder Alert Manager will not start, and Intruder Alert records the following entry in the manager.log file:

```
<path>\ita\system\<hostname>\<number>.rex is encrypted with a
different algorithm.
```

This entry indicates that some or all of the data in the .rex file is corrupted. There is no way to recover data from a corrupted event file. To continue to record current events, use one of the following methods:

- Delete the .ext and .rex files from the <hostname> directory. Restore older .ext and .rex files from the most recent backup. All event data that was recorded since the latest backup will be lost.
- Delete the .ext and .rex files from the <hostname> directory. All event data will be lost.

Because Intruder Alert saves final data to each .rex file before renaming it to an .ext file, .ext files cannot be used to substitute for a corrupted .rex file.

Corrupted .ext files

If Intruder Alert cannot read an .ext file, all events in that file and previous .ext files are lost.

Manage the size of Intruder Alert error logs

Intruder Alert's Manager and Agent record various errors that occur during their operation. Symantec's customer support representatives use these files to diagnose problems. The name of the Manager's error log is "manager.log", and the name of the Agent's log is "agent.log". The default location for these files is in the directory:

<system disk>:\Program Files\Symantec\ITA\system\<hostname>

A setting in the ita.ini file controls the size of these files. The setting is named:

MaxLogSize=

This setting should be adjusted to control the size of each log file (agent, manager, admin, and iview).

The default size is set to 50,000 bytes. When the error log reaches the maximum size specified in the ita.ini file, Intruder Alert saves the file with a .old file extension and builds a new log file with the original file name.

By default, Intruder Alert keeps two archived log files. If a .old error log file already exists, Intruder Alert renames the file to agent/manager.bk1 and creates a new agent/manager.log file. You can manage the number of log files written to the system via the ita.ini file. The default for MaxLog Files is 2. You can set this amount to a maximum of 9,999,999. However, it is not recommended to save more than 10. The size of these logs should depend on how much data you want to keep.

To configure the size of the Intruder Alert error log

1. Open the Agent's ita.ini file in a text editor.
   The file is located in the directory:
   <system disk>:\Program Files\Symantec\ITA\system\<hostname>
2. To modify the size of the Agent's error log, locate the MaxLogSize command under the [Agent] section and specify the new size (in KB).
3. If the Manager resides on the same system as the Agent and you want to modify the size of the Manager's error log, locate the MaxLogSize command under the [Manager Diagnostics] section and specify the new size (in KB).
   Do not use commas or periods. For example:
   MaxLogSize=100000
   MaxLogSize=25000
4. When finished, save the file.
5. Stop and restart the Agent and/or Manager as necessary.
   See "Starting and stopping Managers/Agents" on page 66.

Debug logging

Intruder Alert features an API to control debug logging. It is enabled in the production code, and controls how information is logged in specified modules. All callbacks are identified in the Debug logging code so the operation of the Manager and Agent can be tracked. This helps in identifying and diagnosing policy errors.

Manage the size of UNIX collectors

Process Accounting, syslog, btmp, and wtmp security files will grow indefinitely unless managed. System administrators typically manage the size of these collectors manually. However, Intruder Alert can be configured to automatically truncate these collectors once they reach a certain size. In order for Intruder Alert Administrator to read the new INI file, the Agent and Manager must be restarted. Because the Agent/Manager log file is deleted when the Agent/ Manager is shut down, the Agent Manager Log file resets to zero (0).

More information on how Intruder Alert collects events on UNIX systems is available in Appendix B.

See “UNIX collectors” on page 222.

The automatic truncation feature is configured by adding settings to the Agent’s ita.ini file. There are two settings for each file. Values are entered in kilobytes. Valid entries range between 64 and 8192. If no value is entered, the default is 256 Kilobytes. (Do not use zeros or the letter “K” at the end of the number.)

The first setting enables the first command. The following table lists the activation settings for each collector.

Table D-1 Collector size enabling command

Collector	Command
Process Accounting	ACCT_TRUNC=
syslog	SLOG_TRUNC=
wtmp	WTMP_TRUNC=
btmp	BTMP_TRUNC=

The second setting defines the maximum size of the file.

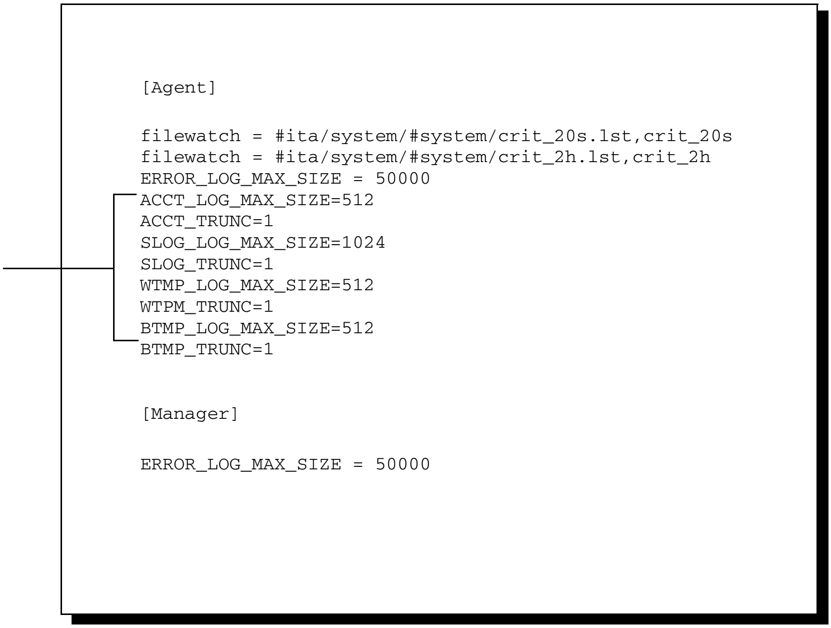
The following table defines this setting for each file.

Table D-2 Collector size commands

Collector	Command
Process Accounting	ACCT_LOG_MAX_SIZE=
syslog (in ITA dir)	SLOG_LOG_MAX_SIZE=
wtmp	WTMP_LOG_MAX_SIZE=
btmp	BTMP_LOG_MAX_SIZE=
C2	C2ATD_START= C2ATD_OPTIONS=

The value 1 enables file truncation, while 0 or a non-existent entry disables file truncation. In the following example, file truncation has been enabled for each collector.

Figure D-1 Modified ita.ini file



```
[Agent]

filewatch = #ita/system/#system/crit_20s.lst,crit_20s
filewatch = #ita/system/#system/crit_2h.lst,crit_2h
ERROR_LOG_MAX_SIZE = 50000
ACCT_LOG_MAX_SIZE=512
ACCT_TRUNC=1
SLOG_LOG_MAX_SIZE=1024
SLOG_TRUNC=1
WTMP_LOG_MAX_SIZE=512
WTPM_TRUNC=1
BTMP_LOG_MAX_SIZE=512
BTMP_TRUNC=1


[Manager]

ERROR_LOG_MAX_SIZE = 50000
```

Add commands to the end of the Agent section.

To configure automatic file truncation on UNIX

1 Open the Agent's ita.ini file in a UNIX text editor.

If Intruder Alert was installed in the default location, the ita.ini file would be located in the axent/ita/system/<hostname> directory.

2 The desired commands are in the Agent section.
See "Modified ita.ini file" on page 266.
Commands are in the ita.ini file, but commented out.

3 When finished, save the file.

4 Stop and restart the Agent.
See "Starting and stopping Managers/Agents" on page 66.
The specified files will automatically be truncated when they reach the specified size.

Optimizing bandwidth usage

Intruder Alert sends packets across the network when:

- Managers update an Agent's configuration (e.g., new policies get added, the Agent is configured with paging or emailing capabilities, etc.)
- Agents send email
- Agents raise global flags
- Agents record event/attack data in the Manager's event database (via the Record to Event Viewer action)

Excessive data crossing the network at one time can hinder data flow. To prevent this problem, Intruder Alert allows you to throttle how much data the Agent sends. However, if you throttle the transfer rate too much, events will accumulate in cache files on the Agent. If these cache files become full, event data may be lost due to a lack of memory to store them.

Intruder Alert offers two throttles to help optimize network bandwidth usage:

- The Record to Event Viewer throttle
- The Send Email throttle

The Record to Event Viewer and Send Email throttles can be configured from within Intruder Alert Administrator. The following sections describe how to configure these throttles.

Configure the Record to Event Viewer action throttle

The Record to Event Viewer throttle defines the rate at which data transfers across the network to the Manager. If the cache file becomes full, Intruder Alert discards low priority events first, replacing them with higher priority events. A low priority event is an event with a low rule value. New events with a lower priority get deleted.

The default throttling speed is set at 5 KB/sec. Set the throttle higher to send more data across the network. If there is a shortage of bandwidth, set the throttle lower, to transfer the data at a slower rate.

To throttle the Record to Event Viewer action

1. From within Intruder Alert Administrator, connect to the desired Manager.
   See “Connecting to a Manager” on page 64.
2. In the Intruder Alert tree, expand the connected Manager’s branch.
3. In the Manager’s branch, expand **Registered Agents**.
4. In the Registered Agents branch, click the desired Agent.
   The Agent’s configuration boxes appear in the right pane.
5. In the Record Action Throttle text box, type the desired throttling value. (The default is 5 KB/sec.)
6. When finished, click **Save**.
   The Record to Event Viewer action is throttled.

Configure the email (SMTP) action throttle

Administrators can reduce the risk of slowing the network by throttling the number of email notification messages the Agent can send per minute. The default limit is 10 emails per minute.

Note: If the number of email messages exceeds the throttle in a given minute, the Agent discards the excessive messages.

To throttle the Send Email action

1. In Intruder Alert Administrator, connect to the desired Manager.
   See “Connecting to a Manager” on page 64.
2. In the Intruder Alert tree, expand the connected Manager’s branch.
3. In the Manager’s branch, expand **Registered Agents**.
4. In the Registered Agents branch, click the desired Agent.
   The Agent configuration boxes appear in the right pane.
5. Click in the SMTP Throttle text box, and enter the desired throttling value. The default value is set to 10 emails per minute.
6. When finished, click **Save**.

Known issues and resolutions

commands.txt changes require system to be restarted

Anytime any Intruder Alert configuration file is changed the Manager must be shutdown and restarted in order for the configuration file to get re-read and implemented. Likewise if changes are made to an Agent configuration file, the Agent must be shutdown and restarted.

A partial list of affected files follow:

- ita.ini
- commands.txt
- uxcrit_L.fio & lst (database file)
- uxcrit_S.fio * lst (database file)
- itaobj.dat

Configuring the maximum record count

In Windows, the maximum record count is preset to a default of 15000. In UNIX it is preset to 1000. This setting prevents the files from consuming disk space and memory. It may be necessary to adjust the setting to suit a particular system. The maximum record setting that triggers the following pop-up notification in Intruder Alert View “Maximum record count reached,” is configurable in the ita.ini file.

To change the setting parameters

1. For Windows, open ita.ini in Notepad or a similar text editor and locate the following setting:
   ```
   [GUI]
   # Specifies the maximum records that each text view can have
   VIEWRECORDS = 15000
   ```
2. Adjust the view record setting to suit the system.
3. Shutdown and restart the Agent.
4. For UNIX, open ita.ini in a text editor and locate the following setting:
   ```
   [GUI]
   VIEWRECORDS = 1000
   ```

Understanding Intruder Alert network traffic

Intruder Alert packets are relatively small. Most policies are less than 1KB in size, so from the Manager to the Agent there is not much traffic. However there are some exceptions. If a particular policy is large, the packet will be bigger. The information passed from Agent to Manager is mostly event data. Most events are less than 500 bytes, but some events can be bigger. Larger packet size will also occur at Agent registration.

From GUI to Manager, packets are usually small (less than 500 bytes), and consist mainly of policy/configuration changes. However from the Manager to the GUI, packets tend to run larger. For example, when the GUI first connects, the Manager transfers over the entire configuration database consisting, on an average, of about 250KB to 1MB of data.

This data is transferred over in 500-byte blocks. An Intruder Alert Event Viewer query can generate a high volume of data across the network. It is not unusual for transfers at 10K-75K a second to occur as the Manager queries historical data. Normal "real-time" event data is usually closer to 2K-5K a second, but once again the file transfer rate varies greatly based on the amount of traffic at a particular installation.

Manager status during tune-up process

Depending upon your network configuration, network traffic, the number of Agents in a domain (connected to a single manager), and available bandwidth; the tune-up process may take 15 minutes to 24 hours or more. During this time the Manager's attention is consumed by the task at hand (the Tuneup application) and it is generally unavailable for other Intruder Alert tasks.

Symantec recommends applying the tune-up pack to no more than 10 Agents (or a domain comprised of 10 Agents or less) at a time.

Tuneup utility requirements for update functionality

Symantec has provided the Tuneup utility to update old agents up to the current release. In order for the Tuneup utility to update the Agent on an NT 4.0 machine, the machine must be using Service pack 5.

Service control error - unable to start service

If you get this error after installing Intruder Alert, you may correct the error by reinstalling the current Service Pack that is running on your Windows system.

TUNEUP fails to upgrade a remote agent

On some systems, Tuneup will not execute a batch job to execute the tune-up file. It creates the /transfer directory and the launch script, but fails to execute. This is most likely an end-user configuration problem.

Tuneup requires that the agent being upgraded have permission to submit the batch job to the operating system. This means that the username of the agent process must be listed in the at.allow file or *not* listed in the at.deny file on the Agent system. On most systems the username will be “root”. However, to ensure the correct username, you can run the following command:

```
ps -ef | grep itaagtd
```

If the username of the itaagtd process is not listed in the at.allow file, if the at.allow file does not exist, or the username is listed in the at.deny file, the agent will not able to start the upgrade process. Either add the username to the at.allow file, or remove it from the at.deny file.

The following is the location list of the at.allow and/or at.deny files on supported operating systems. The list is not comprehensive and cannot anticipate a change in location on a new release of a given operating system. See the 'batch' man page for further details.

AIX	/var/adm/cron
HP-UX 10.20	/var/adm/cron
HP-UX 11i v1 (B.11.11)	/usr/lib/cron
HP-UX 11i v1.5 (B.11.20)	/usr/lib/cron
HP-UX 11i v1.6 (B.11.22)	/usr/lib/cron
HP-UX 11i v2 (B.11.23)	/usr/lib/cron
IRIX	/usr/lib/cron
NCR	/etc/cron.d
OSF1	/usr/lib/cron
Sequent	/usr/lib/cron
Solaris	/usr/lib/cron

Appendix E

SNMP for Intruder Alert

Overview

The SNMP feature in Intruder Alert allows you to configure Intruder Alert to send and receive SNMP messages. You can configure SNMP to forward security events to network management systems, as well as monitor external applications. This capability significantly extends Intruder Alert's ability to manage an enterprise system's security environment.

SNMP for Intruder Alert can be installed and configured to run on Windows.

To send SNMP messages, you must install SNMP, install and configure the IA Query Event Management System, and set up an iaquery user account in Intruder Alert.

To receive SNMP messages, you must configure snmptrap and configure Intruder Alert to receive SNMP traps.

Installing SNMP for Intruder Alert

SNMP for Intruder Alert is installed by running the setup.exe file in the microsft/winnt/intel/snmp directory on the ITA program CD.

To install SNMP for Intruder Alert on Windows:

1. In the microsft/winnt/intel/snmp directory on the ITA program CD, double-click the setup.exe file.
2. Follow the instructions to complete the installation.

The process installs a number of files.

See "SNMP for Intruder Alert installed files" on page 284.

To uninstall SNMP for Intruder Alert, remove SNMP for Intruder Alert through the Add/Remove Programs option in the Windows Control Panel.

Installing the IA Query Event Management Service

The IA Query Event Management Service, which is also referred to as IA Query, is a Windows Service that filters, forwards, and stores security events detected by Intruder Alert.

IA Query can forward Intruder Alert events that occur during a user-specified time period, or it can forward events continuously as they occur in real time.

You can configure IA Query to store security event information in a file to be used by third-party report applications. You can also use IA Query from the command prompt to generate a static report.

Refer to the Installing the IA Query Event Management Service topic in the *IA Query Event Management Service Implementation Guide* for instructions. This document is in the doc directory on the ITA program CD.

Configuring the IA Query Event Management Service

You must configure the Intruder Alert IA Query Event Management Service to allow you to send SNMP traps to a management framework (such as HP OpenView, IBM's Tivoli Enterprise Manager, or Micromuse's Netcool).

Refer to the Creating the Configuration File topic in the *IA Query Event Management Service Implementation Guide* for instructions. This document is in the doc directory on the ITA program CD.

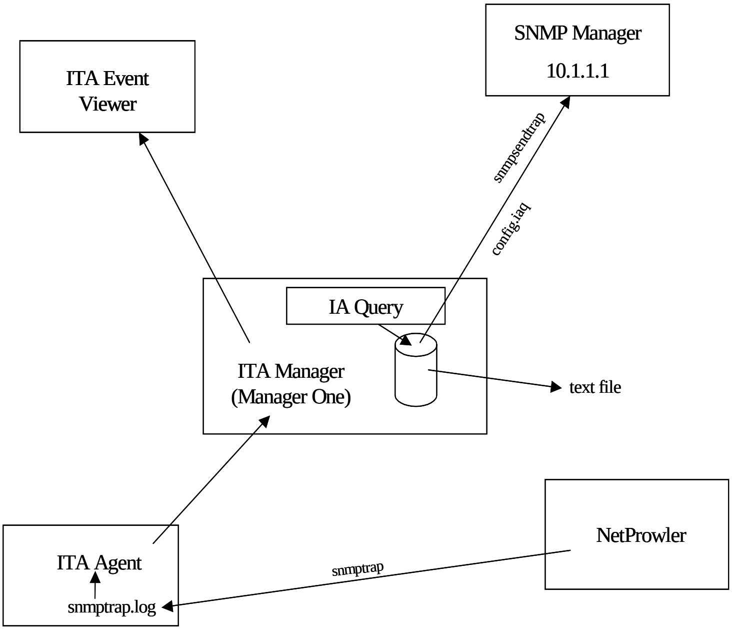
Sample IA Query configuration file

The following file is an example of how to set up the IA Query Event Management Service configuration file. This configuration file shows how IA Query can call a program to send each event as an SNMP trap to an SNMP management station.

```
query_port=3836

output=command


command=c:\progra~1\symantec\ita\bin\snmpsendtrap localhost public
enterprises.axent localhost 6 11 99999 \

intruderalertagentlabel s "%agent%" intruderalerteventtime t
%eventtime% \

intruderalerttrapmessage s "%text%" intruderalerttrapseverity i
%severity% \

agenthostip s "%agent_ip%" policy s "%policy%" \
rule s "%rule%"

poll_interval=1

managers=Manager One
mgr_port=5051
user=iaquery
password=iaquery
query=(*)
mode=real_time
```

Figure E-1 is an example of how SNMP messages are sent to an SNMP Manager and how SNMP messages are received from NetProwler.

Figure E-1 Sample SNMP for Intruder Alert implementation



Adding IAQuery to the ITA User Manager

In the ITA Administrator program, you must add an account to the ITA User Manager to allow IA Query to read events from the ITA database.

The ITA user account that IA Query uses can only have the View Event Information privilege enabled. If additional privileges are enabled for this account, IA Query will not function and this will be logged in the iaquery.log

To add IAQuery to the ITA User Manager:

1 In the Intruder Alert tree, click the desired Manager.

2 On the menu bar, click **Manager > Security > User Manager**.

3 In the User Manager dialog box, click **Add**.

4 Under User Configuration, check the View Event Information check box.

5 In the User Name box, type the user name as specified in the config.iaq file.

6 In the Full Name box, type:

```
iaquery
```

7 In the Password box, type the password as specified in the config.iaq file.

8 In the Confirm Password box, retype the password.

9 Click **Commit**.

Sending SNMP traps

Using the snmpsendtrap.exe executable and the IA Query Event Management Service, you can send SNMP traps of Intruder Alert events as they occur or within a user-specified time period to any SNMP Manager or write the events to a file. An example of an IA Query configuration file that will enable sending of SNMP traps is provided in the section:

See “Sample IA Query configuration file” on page 274.

Note: You must install and configure the IA Query Event Management Service to send SNMP traps of Intruder Alert events to an SNMP Manager. Refer to Installing the IA Query Event Management Service and Creating the Configuration File in the *IA Query Event Management Service Implementation Guide* for instructions. This document is in the doc directory on the ITA program CD.

The syntax for sending SNMP traps is as follows:

```
snmpsendtrap.exe [options...]<hostname><community>[trap parameters]
```

Command line options

The command-line options for snmpsendtrap.exe are described in the following tables.

Table E-1 Options for snmpsendtrap

Option	Description
-h	Display startup options
-H	Display configuration directives
-V	Display version of SNMP supported

Table E-2 General communication options for snmpsendtrap

General communication option	Description
-p <P>	Use port P instead of the default port.
-T <LAYER>	Use LAYER for the network layer (UDP or TCP).
-t <T>	Set the request timeout to T.
-r <R>	Set the number of retries to R.

Table E-3 Debugging options for snmpsendtrap

Debugging option	Description
-d	Dump input/output packets.
-D all | <TOKEN[,TOKEN,...]>	Turn on debugging output for the specified TOKENs.

Table E-4 General options for snmpsendtrap

General option	Description
-o <FILENAME>	Write output to FILENAME. The default output file is snmp.log. Use “-o stdout” to print to screen.
-m | all <MIBS>	Use MIBS list instead of the default MIB list.
-M <MIBDIRS>	Use MIBDIRS as the location to look for MIBs.
-P <MIBOPTS>	Toggle various defaults controlling MIB parsing. MIBOPTS can have the following values: u - Allow the usage of underlines in MIB symbols. c - Disallow the usage of “--” to terminate comments. d - Save MIB object descriptions. e - Disable MIB errors of MIB symbols conflicts. w - Enable MIB warnings of MIB symbols conflicts. W - Enable detailed warnings of MIB symbols conflicts. R - Replace MIB symbols from latest module.
-O <OUTOPTS>	Toggle various defaults controlling output display. OUTOPTS can have the following values: n - Print object IDs numerically. e - Print enumerations numerically; labels associated with enumerations are not printed. b - Do not break down object ID indexes. q - Quick print for easier parsing. f - Print full object IDs on output. s - Print only the last symbolic element of an object ID. S - Print MIB module ID plus the last element.
-I <INOPTS>	Toggle various defaults controlling input parsing. INOPTS can have the following values: R - Randomly access object ID labels. b - Perform best/regex matching to find a MIB node.

The other options are described below:

- <hostname> - The name of the host the trap is being sent from. This can be in the form of a machine name or an IP address.
- <community> - The SNMP Community Name. A Community is a relationship between an SNMP Agent and a set of Managers that defines authentication, access control and proxy characteristics. Each community has a unique name.
- [trap parameters...] - The various parameters required to send the trap to the SNMP Manager. The parameters are described in the following table.

Table E-5 Trap parameters for snmpsendtrap

Parameter	Description
enterprise-oid	The enterprise object ID.
agent	The name of the SNMP Agent sending the trap.
trap-type	The trap-type number. This will always be set to 6.
specific-type	The specific-type number. This will always be set to 11.
uptime	A numeric value which indicates to the SNMP Manager how long the Agent has been up.
[variable bindings...]	Variables which can be described to be sent to the manager. Those variable bindings are: ■ intruderalertagentlabel ■ intruderalerteventtime ■ intruderalerttrapmessage ■ intruderalerttrapseverity ■ agenthostip ■ policy ■ policydescr ■ rule ■ ruledescr

Receiving SNMP traps

You can use SNMP for Intruder Alert to receive SNMP traps and respond to them like any other security event in Intruder Alert. To enable Intruder Alert to receive SNMP traps, you must perform the following tasks:

- Install and configure snmptrap

- Configure Intruder Alert to receive SNMP traps

This section also describes applicable command-line and configuration file options for snmptrap.

Starting snmptrap

To install and start snmptrap

1. At a command prompt, go to the \symantec\ITA\bin directory and type:
   `snmptrap install`
   This will install snmptrap as a Windows service.
2. To start snmptrap, do one of the following:
   - At the command prompt, type:
     `snmptrap start`
   - In the Windows Services window, click the ITA SNMP Trap Collector Service.

Configuring Intruder Alert to receive SNMP traps

To enable Intruder Alert to receive SNMP traps that are collected on an Agent, set up an audit log in the Agent configuration.

To set up an audit log to collect SNMP events

1. In the tree view of Intruder Alert Administrator, expand the desired Manager branch.
2. In the Manager's branch, expand **Registered Agents**.
3. In the Registered Agents branch, click the desired Agent.
4. In the right pane, under Audit Logs, click **New**.
5. In the Audit Log dialog box, in the Description text box, type a description for the audit log, such as:
   `SNMP Audits`
6. In the File Name text box, type `\n\n`.
7. Click **Multiple Line**.
8. In the Strings to Parse text box, type an open double quote and close double quote (“”).
9. Click **OK**.
   Intruder Alert is configured to receive SNMP traps.

Command line options for snmptrap

The command line options for snmptrap are described in the following tables.

Table E-6 Help options for snmptrap

Help option	Description
-h	Display startup options
-H	Display configuration directives
-V	Display version of SNMP supported

Table E-7 Service control options for snmptrap

Service control option	Description
install	Install the snapdragon daemon as a service
start	Start the snapdragon daemon
stop	Stop the snapdragon daemon
remove	Remove the snapdragon service

Table E-8 Startup options for snmptrap

Startup option	Description
-p port	Local port to listen from
-P <filename>	Print received traps to the specified file
-u <PIDFILE>	Create PIDFILE with process id
-s	Log syslog (not supported on Windows)
-l [D0-7]	Set syslog facility to log diamond], log local 0<default> [1-7]
-d	Dump input/output packets
-a	Ignore authentication failure traps
-c CONFFILE	Read CONFFILE as a configuration file
-C	Don’t read the default configuration files

Table E-8 Startup options for snmptrap

Startup option	Description
-m <MIBS>	Use MIBS list instead of default MIB list
-M <MIBDIRS>	Use MIBDIRS as the location to look for MIBS.
-O <OUTOPTS>	Toggle various defaults controlling output display. OUTOPTS values: n Print object IDs numerically. e Print enumerations numerically - labels associated with enumerations are not printed. b Don’t break down object ID indexes. q Quick print for easier parsing. f Print full object IDs on output. s Print only the last symbolic element of an object ID. S Print MIB module ID plus the last element.

Additional utilities

There are several utilities that allow you to manage Intruder Alert’s SNMP communication. These utilities are:

- snmpset - an SNMP application that uses the SET Request to set information on a network entity.
- snmpget - an SNMP application that uses the GET Request to query for information on a network entity.
- snmpgetnext - an SNMP application that uses the GET NEXT request to query for information on a network entity.

Note: To see the available command-line parameters for these utilities, run the respective utility with a -H startup option. To see the available options for the configuration file, run the respective utility with a -h startup option.

Sample configurations

This section describes two specific ways SNMP for Intruder Alert can be used:

- Using SNMP for Intruder Alert to receive SNMP traps from Symantec NetProwler
- Using SNMP for Intruder Alert to send SNMP traps to an SNMP-capable entity.

Receiving SNMP traps from NetProwler

Integrating NetProwler with Intruder Alert provides a multi-tiered intrusion defense strategy. NetProwler's network-based intrusion detection approach and Intruder Alert's multi-platform, host-based detection approach complement each other.

Deploying both solutions together mitigates risk and provides the best possible security for your enterprise. NetProwler -Intruder Alert integration is made possible via Simple Network Management Protocol (SNMP) traps. The NetProwler Agent detects an attack and sends an SNMP trap to an Intruder Alert system. The Intruder Alert SNMP Collector, a service you must install on the Intruder Alert system, receives the trap and translates it into a format the Intruder Alert Agent can read. The Agent then processes the trap and performs the configured actions.

To configure Intruder Alert to receive SNMP traps from NetProwler

1. Configure snmptrap to allow Intruder Alert to receive SNMP traps.
   See "Receiving SNMP traps" on page 279.
2. If you are using an earlier version of Intruder Alert than 3.5, import the NetProwler Integration Policies into the Intruder Alert Policy Library.
   See "Importing NetProwler policies" on page 285..
3. Apply the NetProwler Policies to a NetProwler Domain.

Sending SNMP traps to an SNMP Manager

Using SNMP for Intruder Alert and IA Query, you can send Intruder Alert events from any Intruder Alert Agent to an SNMP Manager. This includes management frameworks such as HP OpenView, IBM's Tivoli Enterprise, and Micromuse's Netcool.

To send a trap to an SNMP Manager:

1. Install SNMP for Intruder Alert.

2 Configure the config.iaq file to send traps to the specified SNMP Manager.

3 Set up a user account for IA Query in the Intruder Alert Administrator.
See "Sending SNMP traps" on page 276.

SNMP for Intruder Alert installed files

The following table lists the files and directories created when SNMP for Intruder Alert is installed on Windows.

Table E-9 Installed files on Windows systems

File / Directory	Description
\ita\mibs	Directory for MIB files
\ita\mibs\IntruderAlertMIB.txt	Intruder Alert Trap Definitions
\ita\mibs\itinasd.mib	NetProwler Trap Definitions
\ita\mibs\RFC1155-SMI.mib	Standard MIB declaration
\ita\mibs\RFC-1212.mib	Standard MIB declaration
\ita\mibs\RFC1213-mib.mib	Standard MIB declaration
\ita\mibs\RFC-1215.mib	Standard MIB declaration
\ita\mibs\SNMPV2-SMI.mib	Standard MIB declaration
\ita\bin	Directory for Intruder Alert executables
\ita\bin\snmpget.exe	Performs an SNMP GET request from an SNMP managed node
\ita\bin\snmpgetnext.exe	Perform an SNMP GET NEXT request from an SNMP managed node.
\ita\bin\snmpset.exe	Performs an SNMP SET request on an SNMP managed node
\ita\bin\snmpsendtrap.exe	Sends an SNMP trap to an SNMP management station
\ita\bin\snmptrap.exe	Installs a service that receives SNMP traps from managed nodes

Note: The \ita\bin directory is created when the Intruder Alert Agent is installed. However, installing SNMP for Intruder Alert adds the files listed in Table E-9 to that directory.

Importing NetProwler policies

The NetProwler-Intruder Alert integration policies are included with the Intruder Alert 3.6 Policy Library. They are also included on the NetProwler 3.5 CD-ROM and are available for download from the Symantec Web site.

If you do not have the Intruder Alert version 3.6 or above, you must import these policies into the Intruder Alert Manager and apply them to the Agent where the Intruder Alert SNMP Collector resides.

Integration policies are saved with a .pol file extension. They can be imported into the Policy Library or a Manager's Policies branch.

To import an integration policy

1. In the Intruder Alert Administrator, connect to the Intruder Alert Manager.
2. Do one of the following:
   - Click **Policy Library**
   - In the Manager's branch, click **Policies**.
3. On the menu bar, click **File > Import Policy**.
4. In the Importing Policies dialog box, select the path and filename.
5. Click **Open**.
6. Repeat steps 2–4 for the other integration policies.
   The integration policies are imported and stored under the selected branch.

Troubleshooting SNMP for Intruder Alert

Intruder Alert Events are not sent to the specified SNMP Manager.

SNMP Manager address in IA Query configuration file

You must configure the IA Query Event Management Service to be able to send SNMP messages to an external SNMP Manager. In the IA Query configuration file, you must specify the IP address of the SNMP Manager to which you want to send Intruder Alert events. Ensure that the IP address you want to send events to is specified in the command parameter.

See "Sample IA Query configuration file" on page 274.

Mode parameter in IA Query configuration file

You may not see the Intruder Alert events you expect on the specified SNMP Manager if the Manager-specific mode parameter is set to history.

When mode=real_time, the Manager selects messages that occur from the current time and forwards them indefinitely.

When mode=history, only events that occur between the specified times are forwarded. You must specify a beginning time and an ending time using the begin and end parameters. This format uses 24-hour time designations.

begin=mmddyyyyhhmm

end=mmddyyyyhhmm

Intruder Alert events are not sent as specified

When the output=command in the IA Query configuration file, ensure that the path for the system command is correct. If the path is incorrect, snmpsendtrap will not run and no events will be forwarded as specified in the configuration file.

Destination ports for Intruder Alert

Overview

Intruder Alert components such as Administrator, Event Viewer, Agents, IA Query, and Tuneup, communicate over the network with the Intruder Alert Manager. When a firewall device is positioned between the components and the Manager, the components must connect to the Manager through the firewall. You must configure the firewall to allow connections initiated from the component systems to reach the Manager on certain ports.

This appendix documents the ports to enable to allow Intruder Alert to pass traffic through your firewall. You must make the required ports known to the firewall by creating protocols and rules, and configuring Network Address Translation (NAT).

For more information about configuring Intruder Alert with a firewall, see the *Intruder Alert 3.6.1 Installation Guide*.

Note: In all situations, the Agents must have the ability to communicate directly with the Managers. This means that TCP/IP connectivity and routing must be configured to allow this communication. This is especially important when the Agent computer is outside of a firewall in a DMZ network and may not otherwise have a route to the assigned IP address of the Manager.

Ports used by Intruder Alert

Normally, source ports are allocated dynamically within the range of 1024-65535. Destination ports have default values in Intruder Alert, but these ports can be changed during installation.

In addition, an Agent can change its destination port during re-registration with a Manager, when using one of the following utilities:

- UNIX: itasetup
- Windows: ITA Mgr-Agt Setup

The following table lists the default TCP destination ports that are used by each component of Intruder Alert.

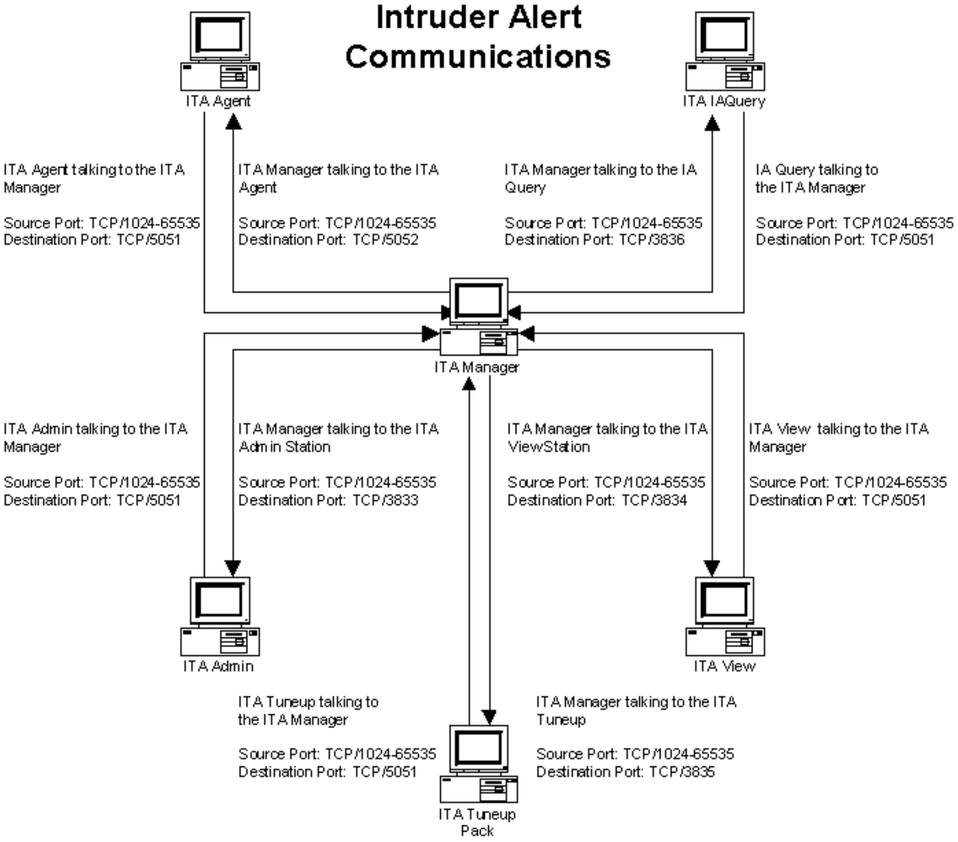
Table F-1 Intruder Alert destination ports

Intruder Alert Component	TCP destination port
Intruder Alert Manager	5051
Intruder Alert Agent	5052
Intruder Alert Administrator	3833
Intruder Alert Event Viewer	3834
Intruder Alert Tuneup	3835
IA Query	3836
Intruder Alert re-registration	2840 (see Note below)

Note: Intruder Alert versions 3.6.1.600 and earlier use destination port 3840 for itasetup and ITA Mgr-Agt Setup. More recent versions of Intruder Alert use port 2840.

The following diagram shows the various Intruder Alert components and the ports used for passing traffic between them.

Figure F-1 Intruder Alert ports and traffic flow


Intruder Alert Communications
ITA Agent
ITA IAQuery
ITA Agent talking to the ITA Manager
Source Port: TCP/1024-65535
Destination Port: TCP/5051
ITA Manager talking to the ITA Agent
Source Port: TCP/1024-65535
Destination Port: TCP/5052
ITA Manager talking to the IA Query
Source Port: TCP/1024-65535
Destination Port: TCP/3836
IA Query talking to the ITA Manager
Source Port: TCP/1024-65535
Destination Port: TCP/5051
ITA Manager
ITA Admin talking to the ITA Manager
Source Port: TCP/1024-65535
Destination Port: TCP/5051
ITA Manager talking to the ITA Admin Station
Source Port: TCP/1024-65535
Destination Port: TCP/3833
ITA Manager talking to the ITA ViewStation
Source Port: TCP/1024-65535
Destination Port: TCP/3834
ITA View talking to the ITA Manager
Source Port: TCP/1024-65535
Destination Port: TCP/5051
ITA Admin
ITA View
ITA Tuneup talking to the ITA Manager
Source Port: TCP/1024-65535
Destination Port: TCP/5051
ITA Manager talking to the ITA Tuneup
Source Port: TCP/1024-65535
Destination Port: TCP/3835
ITA Tuneup Pack

Index